

Fortinet.FCSS\_NST\_SE-7.6.v2026-06-09.q46

|                                                                                                                                                                             |                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Exam Code:                                                                                                                                                                  | FCSS_NST_SE-7.6                              |
| Exam Name:                                                                                                                                                                  | FCSS - Network Security 7.6 Support Engineer |
| Certification Provider:                                                                                                                                                     | Fortinet                                     |
| Free Question Number:                                                                                                                                                       | 46                                           |
| Version:                                                                                                                                                                    | v2026-06-09                                  |
| # of views:                                                                                                                                                                 | 104                                          |
| # of Questions views:                                                                                                                                                       | 484                                          |
| <a href="https://www.freecram.net/torrent/Fortinet.FCSS_NST_SE-7.6.v2026-06-09.q46.html">https://www.freecram.net/torrent/Fortinet.FCSS_NST_SE-7.6.v2026-06-09.q46.html</a> |                                              |

NEW QUESTION: 1

Refer to the exhibit.

```
Routing information

# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
V - BGP VPNv4
> - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S   *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
S   0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S   8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O   10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C   *> 10.0.1.0/24 is directly connected, port3
O   10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C   *> 10.0.2.0/24 is directly connected, port4
B   *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O   *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B   10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C   *> 10.200.1.0/24 is directly connected, port1
C   *> 10.200.2.0/24 is directly connected, port2
```

The modified output of live routing kernel is shown

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

- A. The BGP route to 10.0.4.0/24 is not in the forwarding information base.
- B. The default static route through 10.200.1 254 is in the forwarding information\* base.
- C. FortiGate is performing ECMP using both default static routes.
- D. The local FortiGate is receiving only one LSA from one OSPF neighbor.

Answer: (SHOW ANSWER)

We must analyze the flags (\*, >, S, O, B) and Administrative Distances (AD) shown in the get router info routing-table database exhibit to determine the correct statements.

Analysis for Option A (The BGP route to 10.0.4.0/24 is not in the forwarding information base):

True. Look at the entry for 10.0.4.0/24.

There is an OSPF route: O \*> 10.0.4.0/24 [110/2]. The \* indicates it is in the FIB, and > indicates it is the selected route.

There is a BGP route: B 10.0.4.0/24 [200/10]. This line lacks the \* flag.

Reason: The OSPF route has an Administrative Distance of 110. The BGP route (iBGP) has an AD of 200.

Since 110 is lower than 200, OSPF wins, and the BGP route is not installed in the Forwarding Information Base (FIB).

Analysis for Option B (The default static route through 10.200.1.254 is in the forwarding information base):

True. Look at the 0.0.0.0/0 entries.

The first entry is S \*> 0.0.0.0/0 [10/0] via 10.200.1.254.

The \* flag confirms this specific route is installed in the FIB.

The second static route (via 10.200.2.254) has a higher distance ([20/0]) and no \* flag, so it is inactive.

Why C is False: ECMP (Equal Cost Multi-Path) requires routes to have the same cost/priority. Here, one static route has AD 10 and the other has AD 20. They are not equal, so ECMP is not performed.

Why D is False: The routing table database shows active routes, not the raw Link State Advertisement (LSA) database. You cannot determine the number of LSAs received solely from this output.

Reference:

FortiGate Security 7.6 Study Guide (Routing): "The routing table database displays all known routes... The \* indicates the route is in the FIB... Lower Administrative Distance is preferred."

## NEW QUESTION: 2

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: (SHOW ANSWER)**

IKEv1 (Internet Key Exchange version 1) and IKEv2 are protocols used for establishing IPsec VPN tunnels, and both protocols share the conceptual division into two phases, as clearly described in Fortinet VPN documentation:

Phase 1 handles negotiation and establishment of a secure IKE Security Association (SA) between peers.

Phase 2 negotiates parameters for the IPsec Security Association, which secures actual data traffic between peers.

While IKEv2 streamlines and improves upon IKEv1 by merging some message exchanges and simplifying configuration, it maintains the same core two-phase concept: Phase 1 (IKE SA) and Phase 2 (IPsec SA). This is a foundational VPN concept referenced widely in both IKEv1 and IKEv2 literature.

Other statements are incorrect:

Asymmetric authentication is possible, but not mandatory for both.

Both protocols commonly use UDP port 500, sometimes 4500 for NAT traversal, but they are not designed to run on TCP.

The protocol feature compatibility over TCP/UDP is not correctly described in the other options.

Reference:

FortiOS Administration Guide: IPsec VPN, "IKEv1 vs. IKEv2 Concepts and Phase Negotiations" RFCs and Fortinet VPN solution guides on phase structure

## NEW QUESTION: 3

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

| Server List (Mon May 6 03:47:52 2024) -- |        |     |       |    |                     |       |       |                         |                         |              |
|------------------------------------------|--------|-----|-------|----|---------------------|-------|-------|-------------------------|-------------------------|--------------|
| IP                                       | Weight | RTT | Flags | TZ | FortiGuard-requests | Cur   | Lost  | Total                   | Lost                    | Updated Time |
| 64.26.151.37                             | 10     | 45  |       | -5 | 262432              | 0     | 0     | 846                     | Mon May 6 03:47:43 2024 |              |
| 64.26.151.75                             | 10     | 46  |       | -5 | 329072              | 0     | 0     | 6806                    | Mon May 6 03:47:43 2024 |              |
| 66.117.56.37                             | 10     | 75  |       | -5 | 71638               | 0     | 0     | 275                     | Mon May 6 03:47:43 2024 |              |
| 65.210.95.240                            | 20     | 71  |       | -8 | 36875               | 0     | 0     | 92                      | Mon May 6 03:47:43 2024 |              |
| 209.22.147.36                            | 20     | 103 | D     | -8 | 34784               | 0     | 0     | 1070                    | Mon May 6 03:47:43 2024 |              |
| 208.91.112.194                           | 20     | 107 | D     | -8 | 35170               | 0     | 0     | 1533                    | Mon May 6 03:47:43 2024 |              |
| 96.45.33.65                              | 60     | 146 |       | 0  | 33728               | 0     | 0     | 120                     | Mon May 6 03:47:43 2024 |              |
| 80.85.69.41                              | 71     | 226 |       | 1  | 33797               | 0     | 0     | 192                     | Mon May 6 03:47:43 2024 |              |
| 62.209.40.74                             | 150    | 97  |       | 9  | 33754               | 0     | 0     | 143                     | Mon May 6 03:47:43 2024 |              |
| 121.111.236.179                          | 45     | 44  | F     | -5 | 26410               | 26226 | 26227 | Mon May 6 03:47:43 2024 |                         |              |

In this exhibit, which FDS server will the FortiGate algorithm choose?

- A. 66.117.56.37
- B. 209.22.147.36
- C. 64.26.151.37
- D. 208.91.112.194

Answer: (SHOW ANSWER)

NEW QUESTION: 4

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: (SHOW ANSWER)

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: 5

Exhibit.

```

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.
es_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%
BDEV 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
Cluster 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. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
- D. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

**Answer:** ([SHOW ANSWER](#))

FortiGate HA Troubleshooting and Synchronization Guides

Fortinet Admin Guide: HA Primary Role Retention, Cluster Break-up Due to Out-of-Sync Status

#### NEW QUESTION: 6

In which two states is a given session categorized as ephemeral? (Choose two.)

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

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 7

Refer to the exhibit.

```
Debug output

FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=redir local may_dirty none app_ntf
statistic (bytes/packets/allow/err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
src mac=08:5b:0e: 6c:76:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
src_ip=007.52948 src_if=0 app_list=0 app=0 url_cat=41
reply_ip=00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

Which two statements about FortiGate behavior relating to this session are correct? (Choose two.)

- A. FortiGate is performing a security profile inspection using the CPU.
- B. FortiGate redirected the client to trio captive portal to authenticate so that a correct policy match could be
- C. FortiGate either initiated the session or the session terminates at FortiGate.
- D. FortiGate forwarded this session without any inspection.

**Answer:** (SHOW ANSWER)

Based on the Fortinet FCSS - Network Security 7.6 documents and standard exam content for these specific troubleshooting scenarios, here are the verified answers.

Questions no: 74

Verified Answer: A, C

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

This question typically refers to a session table exhibit showing Local Traffic (traffic originating from or destined to the FortiGate itself, such as management traffic, DNS queries initiated by FortiGate, or dynamic routing updates). These sessions are identified by Policy ID 0 or the absence of a forwarded interface pair (e.g., local flag).

C). FortiGate either initiated the session or the session terminates at FortiGate:

This is the definition of Local Traffic. Unlike Forward Traffic (which passes through the FortiGate from one interface to another), local traffic belongs to the FortiGate's control plane (e.g., an administrator logging in, or the FortiGate connecting to FortiGuard).

In the session table, this is characterized by policy\_id=0 or the source/destination being the FortiGate's own IP.

A). FortiGate is performing a security profile inspection using the CPU:

Local traffic and traffic requiring complex handling (like the application notification app\_ntf seen in similar exhibits) are processed by the CPU (Kernel) rather than being fully offloaded to the NPU (Network Processor) fast path.

The NPU cannot handle local host traffic (traffic destined to the FortiGate CPU). Therefore, the CPU must process these packets.

Why other options are incorrect:

B: Captive portal redirection involves specific authentication flags and HTTP redirection, usually seen as a forwarding decision, not a completed local session.

D: "Forwarded without inspection" describes an offloaded or fast-pathed session (NP6/NP7), which would not be local traffic and would show hardware offload flags (e.g., np6\_0).

Reference:

FortiGate Security 7.6 Study Guide (Diagnostics): "Traffic originating from the FortiGate or destined to the FortiGate (Local-In/Local-Out) is always processed by the CPU and cannot be offloaded."

NEW QUESTION: 8

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 BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
- C. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.
- D. The router ID of the neighbor is 100.64.2.254.

Answer: (SHOW ANSWER)

NEW QUESTION: 9

Refer to the exhibits.

Exhibit 1

```
FGT-A # get router info bgp summary
...

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4      65110   2500   2552      5      0      0 1d11h33m      0
```

Exhibit 2

```
FGT-B # show router bgp

config network
edit 1
set prefix 172.16.0.0 255.255.0.0
next
end
```

Exhibit 3

```
FGT-B # diagnose ip address list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.

Which two actions can the administrator take to fix this problem? (Choose two.)

- A. Use the set network-import-check disable command.
- B. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
- C. Manually add the BGP route on FGT-A.

D. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 10

Refer to the exhibit.

```
FGT-01
#diagnose sniffer packet any 'esp' 4
2024-03-07 15:57:40.344931 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415b)
2024-03-07 15:57:40.344949 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415c)
2024-03-07 15:57:40.344974 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415d)
2024-03-07 15:57:40.346832 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415e)
2024-03-07 15:57:40.347463 port1 out 42.123.56.38 -> 97.86.16.52: ESP(spi=0xe8f9b3cf,seq=0x1e3415f)

FGT-02
#diagnose sniffer packet any 'esp' 4
(no packets captured)
```

The sniffer log on two FortiGate devices are shown. Based on the information in the log, which two factors explain the output on FortiGate FGT-02? (Choose two answers)

- A. A third-party device is blocking protocol 50.
- B. The administrator has not yet configured the VPN tunnel on FGT-02.
- C. The administrator configured the wrong remote peer IP address on FGT-01.
- D. The administrator set the wrong sniffer filter on FGT-02.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Network Security

7.6 documents:

The output on FGT-01 confirms that the device is actively encapsulating traffic and sending it as ESP packets (Protocol 50) out of port1 towards the IP address 97.86.16.52. The logs show outgoing packets, which confirms FGT-01 is attempting to initiate or maintain the tunnel and that NAT-Traversal is not being used (as it uses raw ESP).

The output on FGT-02, however, displays (no packets captured). This is significant because the sniffer command `diagnose sniffer packet any 'esp'` captures traffic at the network interface level (ingress), regardless of whether a matching VPN configuration exists on the receiving unit. The absence of packets proves that the ESP traffic generated by FGT-01 is physically not arriving at FGT-02's interface.

This behavior is explained by two primary factors:

\* Option A (Blocking): An intermediate device, such as an ISP router or firewall, is dropping Protocol 50 traffic. Unlike UDP 500/4500, raw ESP is often blocked by default on many networks or legacy devices.

\* Option C (Routing/Misconfiguration): If the administrator configured the wrong remote peer IP on FGT-01, the packets are being routed to a different destination entirely. Consequently, they never arrive at FGT-02 to be captured.

Option B is incorrect because even without a configured VPN tunnel, the sniffer would still display the incoming ESP packets if they were reaching the interface. Option D is incorrect because FGT-01 is sending ESP, making 'esp' the correct filter.

#### NEW QUESTION: 11

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
[fssod_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: ([SHOW ANSWER](#))

<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: 12

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

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 13

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_FCDN-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. FortiOS performs a bind to the LDAP server using the user's credentials.
- B. FortiOS collects the user group information.
- C. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

D. The user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 14

What are two reasons you might see iprope\_in\_check() check failed, drop when using the debug flow?

(Choose two.)

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

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 15

What are two reasons you might see iprope\_in check () check failed, drop when using the debug How?

(Choose two.)

- A. The packet was dropped because it is not allowed by any firewall policy.
- B. The packet was dropped because there is no route to the source.
- C. The packet was dropped because the trusted host list is misconfigured
- D. The packet was dropped because the requested service is not enabled on FortiGate

Answer: ([SHOW ANSWER](#))

The debug flow message iprope\_in\_check() check failed, drop specifically indicates a failure in the Local-In Policy check. The "iprope" (IP ROouting Policy Enforcement) engine handles policy lookups. The \_in\_check suffix confirms that the decision is regarding traffic destined to the FortiGate itself (Local-In traffic), rather than traffic passing through it.

D). The packet was dropped because the requested service is not enabled on FortiGate:

This is the most common cause. When a packet arrives destined for the FortiGate's interface IP (e.g., an HTTPS or SSH request), the kernel checks if that specific service is enabled in the interface settings (set allowaccess). If the service is not enabled (e.g., trying to Ping an interface where PING access is disabled), the iprope\_in\_check function fails and drops the packet immediately.

C). The packet was dropped because the trusted host list is misconfigured:

Even if the service (e.g., HTTPS) is enabled on the interface, the FortiGate checks the Administrator settings.

If Trusted Hosts are configured, the source IP of the incoming packet is compared against the allowed list. If the IP is not on the list, the Local-In policy check (iprope\_in\_check) fails, and the packet is dropped to secure the management plane.

Why other options are incorrect:

A: If traffic is dropped by a standard Firewall Policy (traffic passing through the device from one interface to another), the debug message will typically state denied by policy x or no matching policy. It would generally be a forward check (iprope\_fwd\_check or similar), not an \_in\_check.

B: If there is no route to the source, the error is a Reverse Path Forwarding (RPF) failure. The debug flow logs this explicitly as reverse path check fail, drop.

Reference:

FortiGate Troubleshooting Guide (Debug Flow): "The message iprope\_in\_check() check failed indicates the packet was denied by the Local-In policy. This occurs when traffic destined to the FortiGate is not allowed by the allowaccess configuration or is blocked by Trusted Host settings."

#### NEW QUESTION: 16

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-time FSSO debug.
- D.** The heartbeat messages must be manually enabled on FortiGate.

**Answer: B,C (LEAVE A REPLY)**

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.

References:

Technical Tip: Useful FSSO Commands (Fortinet Community)

FortiOS Administration Guide: FSSO, Collector Agent, Heartbeat, CLI Debug

**Valid FCSS\_NST\_SE-7.6 Dumps** shared by EduDump.com for Helping Passing FCSS\_NST\_SE-7.6 Exam! EduDump.com now offer the **newest FCSS\_NST\_SE-7.6 exam dumps**, the EduDump.com FCSS\_NST\_SE-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCSS\_NST\_SE-7.6 dumps with Test Engine here:

[https://www.edudump.com/exams/Fortinet/FCSS\\_NST\\_SE-7.6/premium/](https://www.edudump.com/exams/Fortinet/FCSS_NST_SE-7.6/premium/) (133 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### **NEW QUESTION: 17**

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A.** diagnose sniffer packet any 'udp port 500'
- B.** diagnose sniffer packet any 'ip proto 50'
- C.** diagnose sniffer packet any 'udp port 4500'
- D.** diagnose sniffer packet any 'ah'

**Answer: (SHOW ANSWER)**

To capture encrypted IPsec phase 2 (ESP) traffic between two FortiGate devices, the correct protocol filter to use is ip proto 50. According to the Fortinet official sniffing and debugging documentation, ESP (Encapsulating Security Payload) is used for encrypted phase 2 payload transfer and always uses IP protocol number 50. Running the command diagnose sniffer packet any 'ip proto 50' captures only ESP packets, which represent the encrypted traffic-whether originating or transiting the device.

If there is no NAT device between FortiGates, ESP is not encapsulated in UDP (thus not on UDP port 4500; if NAT-T were required, packets would be UDP-encapsulated, but the scenario explicitly says NAT is not in use). UDP port 500 is for IKE control (negotiation) traffic, and AH (Authentication Header, ip proto 51) is not used for encryption in standard IPsec phase 2 with ESP.

This matches the official CLI reference from Fortinet for VPN and traffic analysis.

\*\*

References:

FortiOS CLI Reference: diagnose sniffer packet, ESP, IP Protocol Numbers FortiGate VPN Administration Guide: Traffic Capture and Analysis of IPsec Traffic

### NEW QUESTION: 18

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 authenticated 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
origin->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)
cos/(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
pdpb_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 is being inspected using flow inspection.
- C. The session was initiated from an authenticated user.
- D. The session is being offloaded.

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 19

Exhibit.

```

ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=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 Fortigate/Fartios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C00000000
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 ENCRnone
ike 0: Remotesite:3: type=OAKLEY HASHrpt_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 A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B0000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
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/06b89c022d4df682

```

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: (SHOW ANSWER)**

From the exhibit, you can observe that the debug output captures an IKEv1 negotiation in aggressive mode.

Let's break down the supporting details in line with official Fortinet IPsec VPN troubleshooting resources and debug guides:

For Option B:

The very first line of the debug output shows:

comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.

This indicates the traffic direction-from the remote IP (10.0.0.2) with port 500 to the local IP (10.0.0.1) with port 500. According to Fortinet's documentation, the right side of the arrow always represents the local FortiGate gateway. Thus, 10.0.0.1 is the local gateway IP address.

For Option D:

You see the statement:

negotiation result "remote"

and

received peer identifier FQDNCE88525E7DE7F00D6C2D3C00000000

Official debug documentation describes that the "peer identifier" or peer ID sent by the initiator is displayed here. In the context of IKE/IPsec negotiation, this value is used as the IPsec peer ID for authentication and identification purposes. The initiator is providing "remote" as the peer ID for its connection.

Why Not A or C:

Perfect Forward Secrecy (PFS): The debug does not show any DH group negotiation in phase 2 (no reference to group2, group5, etc., for phase 2), so you cannot deduce the presence of PFS solely from this output.

Phase 2 negotiation: The log focuses on IKE (phase 1) negotiation and establishment; there's no reference to ESP protocol, Quick Mode, or other identifiers that would show phase 2 SA negotiation and establishment.

This interpretation aligns with the explanation in the FortiOS 7.6.4 Administration Guide's VPN section and the official debug command output samples published in Fortinet's documentation. It demonstrates how to distinguish between local and remote addresses and how to identify the use of peer IDs.

References:

FortiOS 7.6.4 Administration Guide: IPsec VPN and Debugging VPNs

Technical Support Resources on interpreting IKE debug output and peer ID roles

### NEW QUESTION: 20

Refer to the exhibit, which shows the output of get router info ospf neighbor.

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID    Pri   State           Dead Time   Address      Interface
0.0.0.1        1     Full/DR         00:00:39    10.10.2.1    wan1
0.0.0.3        1     Full/DROther    00:00:37    10.10.3.2    wan2
0.0.0.10       c1    Full/-          00:00:36    172.16.1.2   ToHub
```

What can you conclude from the command output?

- A. All neighbors are in area 0.0.0.0.
- B. The local FortiGate is the BDR.
- C. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to-point.
- D. The local FortiGate is not a DROther.

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 21

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:** ([SHOW ANSWER](#))

According to Fortinet's LDAP authentication workflow as described in the FortiOS Administration Guide and the official LDAP debug log interpretation, each authentication attempt is split into several key steps: Bind Request, Search Request, and then, if successful, a Bind as the found user DN. In the provided debug output, we see "start search\_dn-base" with a filter "sAMAccountName=jsmith" and the log line "Going to SEARCH state," confirming that FortiOS is in the second step-the Search Request (Option D). Official documentation highlights this exact phrase "SEARCH state" as indicative of Step 2 within the LDAP process ("Bind # Search # Bind").

Additionally, the last line "Found DN 1: CN=John Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet, DC=com" verifies that the system has successfully mapped the username to the Distinguished Name (DN) and this user is "John Smith." The authentication will now proceed using this mapped user (Option B).

Fortinet's logs record the found DN after a successful search, which is a strong confirmation that the user's credentials can be validated against the found DN.

Options A and C are not supported directly by the debug output shown:

The server name "Lab" is referenced as part of the request, but not explicitly as the LDAP server's configured name in this output.

Step 3 (Bind Request) would follow finding the DN, but the log here demonstrates the Search and DN found- per Fortinet, this precedes the actual Bind/validation step.

References:

FortiOS Administration Guide: LDAP Authentication Process and Debug Logs Fortinet Official KB: LDAP Integration Workflow and Log Interpretation

**NEW QUESTION: 22**

Refer to the exhibit.

The output of a BGO debug command is shown.



```
# 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    | 0      | 0   | 0    | never    | OpenSent     |
| 10.127.0.75 | 4 | 65060 | 2206    | 2250    | 102    | 0   | 0    | 02:45:55 | 0            |
| 100.64.3.1  | 4 | 65061 | 101     | 115     | 0      | 0   | 0    | never    | Active       |

Total number of neighbors 3

What is the most likely reason that the local FortiGate is not receiving any prefixes from its neighbors?

- A. The local router is waiting for the keepalive message from the router 10.125.0.60.
- B. None of the three neighbors has successfully established the TCP three-way handshake with the local router.
- C. The router 100.64.3.1 is waiting for the OPEN message from the local router.
- D. The RIB-OUT configuration for router 10.127.0.75 prevents any route advertisement to the local router.

**Answer:** ([SHOW ANSWER](#))

To identify the reason for the lack of prefixes, we must interpret the State/PfxRcd and Up/Down columns in the get router info bgp summary exhibit.

Analyze Neighbor Status:

Neighbor 10.125.0.60: State is OpenSent. This session is not established. It is stuck in the negotiation phase.

Neighbor 100.64.3.1: State is Active. This session is not established. The router is actively trying to initiate a TCP connection.

Neighbor 10.127.0.75:

Up/Down: 02:45:55. This indicates the BGP session has been Up (Established) for almost 3 hours.

State/PfxRcd: 0. This number represents the count of prefixes received. The session is fully established, but the neighbor has sent zero routes.

Determine the Cause:

Since the session with 10.127.0.75 is established, connectivity and handshakes (Options A, B, C) are not the issue for this neighbor.

The fact that it is Up but sending 0 prefixes strongly implies that the neighbor is configured to filter out its routes before sending them to the local FortiGate.

Option D correctly identifies this as a RIB-OUT (Routing Information Base - Outbound) configuration issue on the neighbor (Router 10.127.0.75), which prevents it from advertising its routes.

Reference:

FortiGate Security 7.6 Study Guide (BGP): "In the BGP summary, if the State/PfxRcd shows a number (e.g.,

0), the session is Established. A value of 0 means the peering is up, but no routes have been received, often due to route-map or prefix-list filtering on the remote peer."

### NEW QUESTION: 23

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-rtc 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
nat: 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=1472 esn=0 repl=0 repl_wins=2048
    seqno=1 esn=0 replaywin_lastseq=00000079 in=0 out=0 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 54aac30e29ce711d2ccaab9b5e179c20bb83605e
  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 'esp and host 10.200.3.2'
- B. diagnose sniffer packet any 'host 10.0.10.10'
- C. diagnose sniffer packet any 'ip proto 50'
- D. diagnose sniffer packet any 'port 4500'

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 24

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

- A. The SSL certificate used for FSSO over SSL has expired.
- B. The connection was refused. There may be a mismatch of the TCP port.
- C. FortiGate cannot reach the IP address of the collector agent.
- D. The pre-shared key does not match
- E. The group filters do not match.

Answer: ([SHOW ANSWER](#))

The diagnose debug authd fsso server command is the primary tool for troubleshooting communication between the FortiGate and the FSSO Collector Agent. This debug output reveals the status of the connection and the reasons for failure. The three most common connectivity issues identified by this debug are:

FortiGate cannot reach the IP address of the collector agent (Option C): The debug will show connection timeouts or "host unreachable" errors if the Layer 3 connectivity is missing.

The connection was refused / Port mismatch (Option B): If the FortiGate can reach the IP but the Collector Agent is not listening on the specified port (default 8000), the debug will display "Connection refused." This often happens if the port configured on the FortiGate does not match the listening port on the agent.

The pre-shared key does not match (Option D): If the IP and Port are correct, the next step is authentication. If the password configured on the FortiGate does not match the one on the Collector Agent, the debug will explicitly show an "Authentication failed" or "password mismatch" error during the handshake.

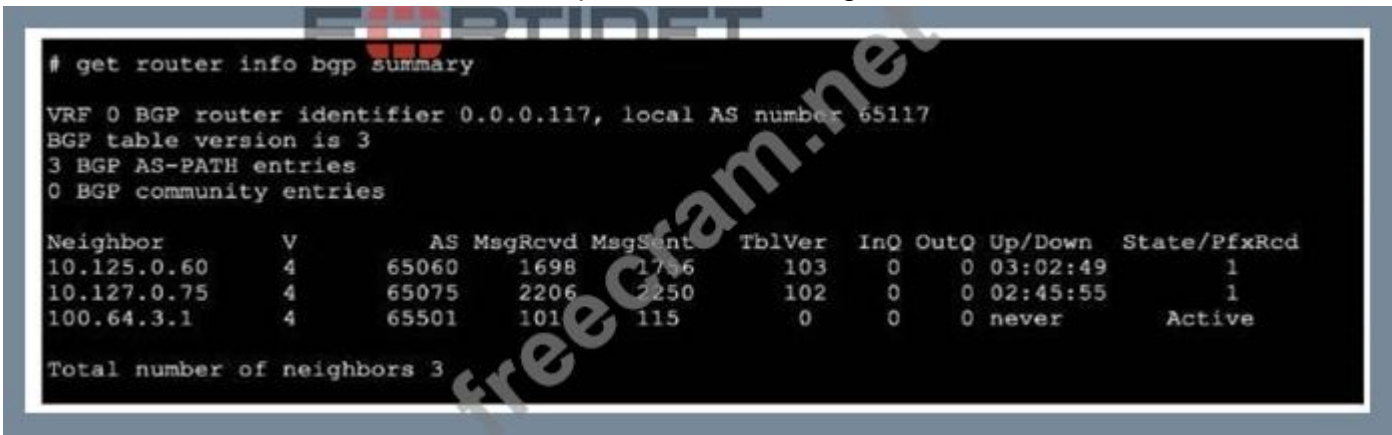
Note on other options: Option A (SSL) is less common than basic connectivity/auth mismatches. Option E (Group filters) relates to user processing logic, which occurs after connectivity is established.

Reference:

FortiGate Security 7.6 Study Guide (FSSO Troubleshooting): "Troubleshooting FSSO... Check connectivity (IP/Port) and authentication (Password)."

**NEW QUESTION: 25**

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



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 BGP 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: (SHOW ANSWER)**

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.

References:

FortiOS BGP Debugging Guide: Session State Interpretation

BGP CLI Reference: Neighbor Status Fields

**NEW QUESTION: 26**

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 to 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:** ([SHOW ANSWER](#))

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.

References:

FortiOS Administration Guide: Session Table, NAT, and Route Interaction Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

## NEW QUESTION: 27

When FortiGate enters conserve mode because of memory pressure, which action can FortiGate perform to preserve memory?

- A. FortiGate automatically reboots to clear memory and restore full operation.
- B. FortiGate switches to a less memory-intensive inspection mode, such as flow-based inspection.
- C. FortiGate reduces or stops non-essential processes like logging and antivirus scanning
- D. Fortigate begins dropping all new sessions to protect resources.

**Answer:** ([SHOW ANSWER](#))

When the FortiGate enters Conserve Mode due to high memory pressure (specifically reaching the Extreme Threshold at 95% memory usage, or the Red Threshold for proxy traffic), the system prioritizes stability and preventing a system crash (kernel panic).

D). FortiGate begins dropping all new sessions to protect resources:

In Extreme Conserve Mode (95%), the FortiGate kernel acts to preserve the remaining memory for system- critical tasks (like admin access and basic packet forwarding of existing sessions). To achieve this, it drops all new session initiation requests regardless of the inspection type.

In Red Conserve Mode (88%), it specifically drops new sessions that require proxy-based inspection (as these consume the most memory), while often still allowing flow-based traffic.

Among the provided choices, "dropping new sessions" is the only standard protective mechanism FortiOS employs to stop memory usage from climbing further.

Why other options are incorrect:

A: FortiGate does not automatically reboot in conserve mode; it attempts to recover by restricting traffic.

(Reboot is a last-resort crash, not a configured action).

B: Inspection modes (Proxy vs. Flow) are defined in firewall policies and cannot be dynamically switched by the system during runtime.

C: The system does not arbitrarily stop "non-essential processes" like logging or AV. Logging is critical for audit trails. While av-failopen can be configured to bypass scanning, the system typically defaults to "Fail- Close" (dropping traffic) rather than stopping the engines themselves.

Reference:

FortiGate Security 7.6 Study Guide (Diagnostics & Resource Usage): "When memory usage reaches the extreme threshold (95%), all new sessions are dropped to prevent memory exhaustion."

### NEW QUESTION: 28

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. Ensure TCP port 8013 is not blocked along the way.

C. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.

D. FortiGate must not be in NAT mode.

E. Ensure the port for Neighbor Discovery has been changed.

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 29

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

A. Refused connection. Potential mismatch of TCP port.

B. Incompatible collector agent software version.

C. Mismatched pre-shared password.

D. Log is full on the collector agent.

E. Inability to reach IP address of the collector agent.

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 30

During which phase of IKEv2 does the Diffie-Hellman key exchange take place?

A. IKE\_Auth

B. IKE\_SA\_INIT

C. IKE\_Req\_INIT

D. Create\_CHILD\_SA

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 31

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

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

Answer: ([SHOW ANSWER](#))

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

**Valid FCSS\_NST\_SE-7.6 Dumps** shared by EduDump.com for Helping Passing FCSS\_NST\_SE-7.6 Exam! EduDump.com now offer the **newest FCSS\_NST\_SE-7.6 exam dumps**, the EduDump.com FCSS\_NST\_SE-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCSS\_NST\_SE-7.6 dumps with Test Engine here:

[https://www.edudump.com/exams/Fortinet/FCSS\\_NST\\_SE-7.6/premium/](https://www.edudump.com/exams/Fortinet/FCSS_NST_SE-7.6/premium/) (133 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### NEW QUESTION: 32

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: ([SHOW ANSWER](#))

The exhibit for question 4 shows a policy route table entry, and key fields are as follows:

internet service(1) : Fortinet-FortiGuard(1245324,0.0.0.0,0.0.0.0)

According to the Fortinet official documentation, when a policy route is based on Internet Service Database (ISDB) entries, the route entry will specifically mention "internet service," showing the service being referenced (in this example, Fortinet-FortiGuard). This is fundamentally different from a regular policy route, which is defined by source, destination, and service wildcards without referencing an ISDB signature. A regular policy route's output would not contain the line "internet service." Policy routes that use ISDB allow FortiGate to steer traffic for specific well-known services (like FortiGuard, Google, Microsoft) based on traffic pattern recognition, even if the destination IP is dynamic. The matching and route selection follow the ISDB tag and can coexist with static or regular policy routes.

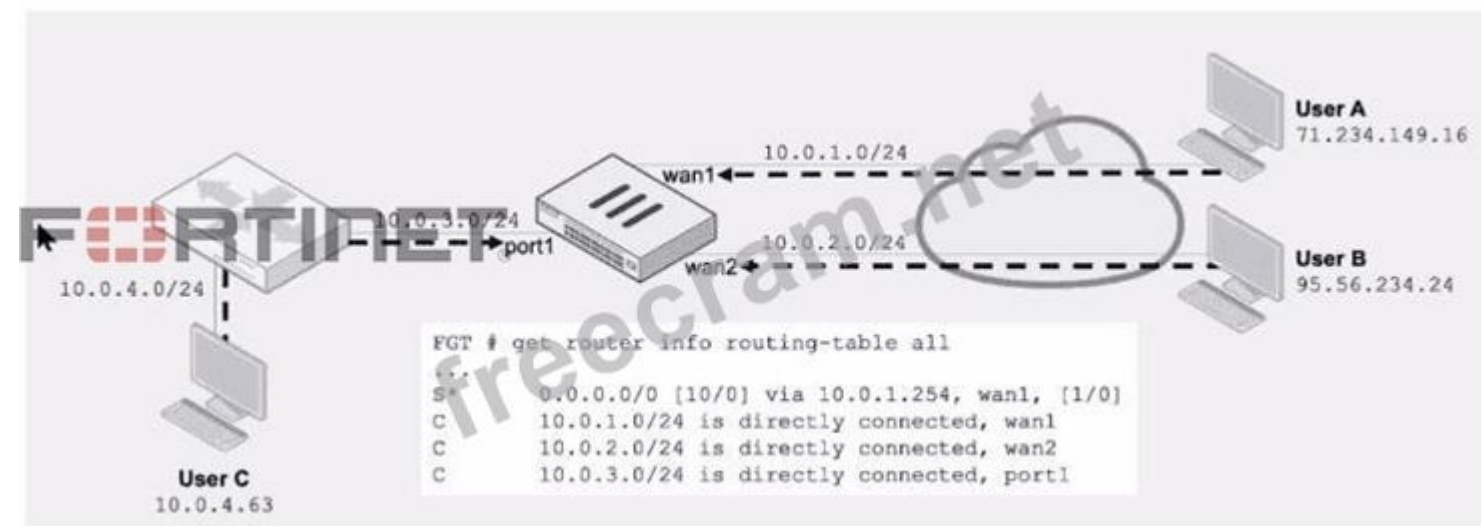
Thus, this entry is correctly and uniquely an ISDB route, as explained in the FortiOS policy routing documentation and ISDB configuration references.

References:

FortiOS Administration Guide: Policy Routing, ISDB integration and interpretation of route table entries ISDB-based Routing and Official CLI Outputs in Fortinet's documentation

### NEW QUESTION: 33

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: Fail. There is no route to 95.56.234.24 using wan2 in the routing table.
- C. User A: Pass. The default static route through wan1 passes the RPF check regardless of the source IP address.
- D. User B: Pass. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
- E. User C: Fail. There is no route to 10.0.4.63 using port1 in the routing table.

**Answer: (SHOW ANSWER)**

References:

Fortinet Technical Note: RPF Default Configuration and Routing Table Matching FortiGate Administration Guide: Routing and Asymmetric Routing Controls Community Knowledgebase: Route Lookups and RPF Enforcement on FortiOS

### NEW QUESTION: 34

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

```
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
```

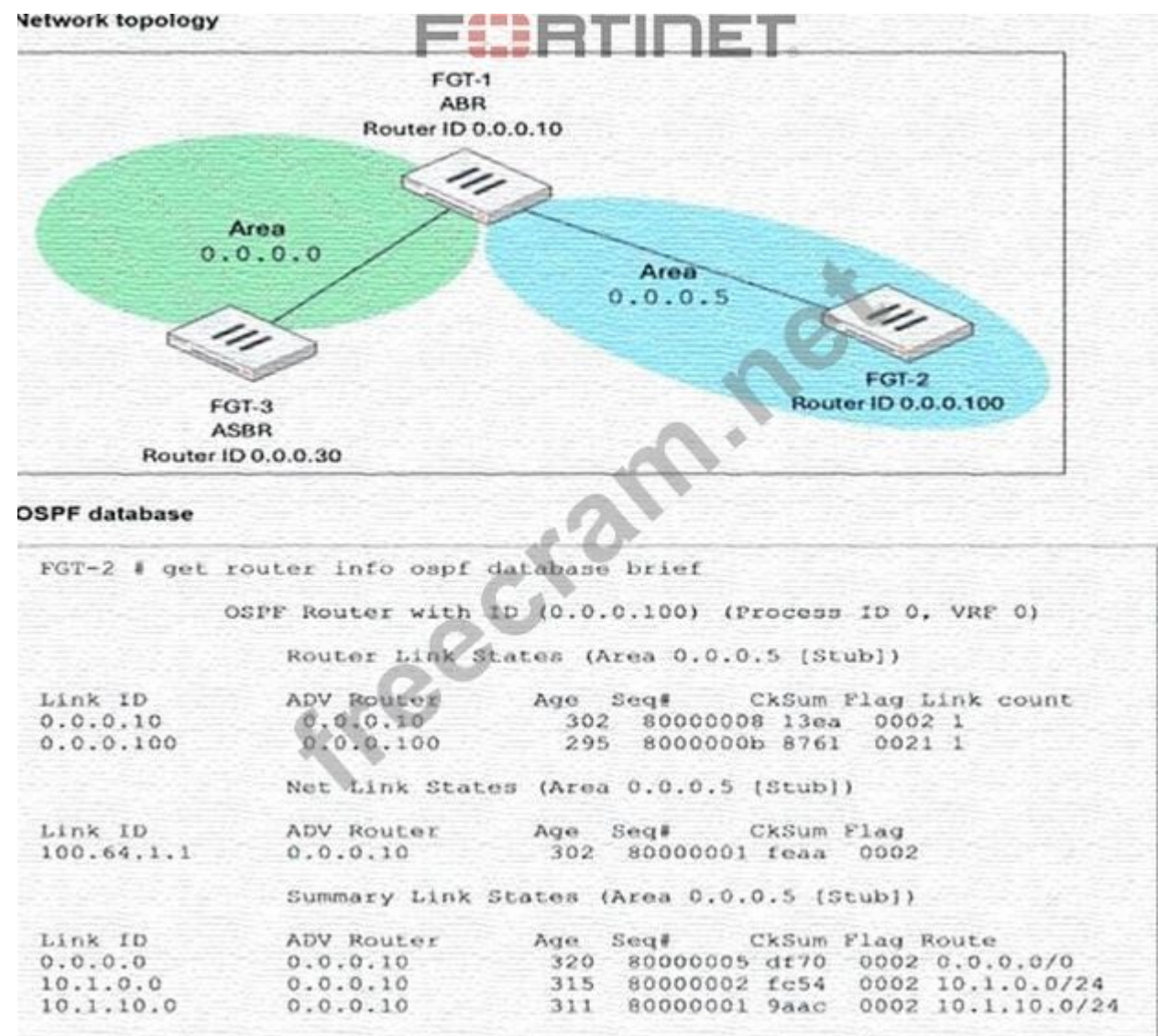
Why are the two FortiGate devices unable to form an adjacency?

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

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 35

While troubleshooting a FortiGate web filter issue, users report that they cannot access any websites, even though those sites are not explicitly blocked by any web filter profiles that are applied to firewall policies.



What are the three most likely reasons for this behavior? (Choose three answers)

- A. The web filter cache has been cleared causing all websites to take longer to be rated.
- B. The SSL/TLS deep inspection was configured but the browsers do not have the FortiGate certificate installed.
- C. The webfilter-force-off setting has been enabled under config system fortiguard.
- D. The DNS server is unreachable, preventing URL resolution.
- E. The FortiGuard Web Filtering license has expired, causing FortiGate to apply the default block action.

**Answer: (SHOW ANSWER)**

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Network Security

7.6 documents:

The reported symptom-users unable to access any websites despite no explicit blocks in the profile-points to systemic connectivity or configuration issues rather than specific URL filtering rules.

\* Option B (SSL/TLS Inspection): When Deep Inspection is enabled, the FortiGate acts as a Man-in-the-Middle (MitM) and re-signs server certificates using its own CA. If the clients (browsers) do not trust this CA (i.e., the certificate is not installed in their Trusted Root store), they will reject the connection with certificate errors, effectively preventing access to all HTTPS websites.

\* Option D (DNS): Web browsing relies on DNS resolution. If the configured DNS server is unreachable or failing, the FortiGate (or the client) cannot resolve FQDNs to IP addresses.

Consequently, browsers will fail to load any page, resulting in a total loss of web access.

\* Option E (License): If the FortiGuard Web Filtering license expires, the FortiGate can no longer query the FortiGuard Distribution Network (FDN) for ratings. By default, or if the allow-when-rating- error setting is disabled (a common security practice), the FortiGate will block all web traffic that it cannot rate, often displaying a "Web Filter Service Error" or invalid license page.

Option A is incorrect because clearing the cache only increases latency, it does not block traffic. Option C is incorrect because webfilter-force-off is typically used to disable the service (often allowing traffic to bypass checks if the service is down), rather than blocking it.

NEW QUESTION: 36

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=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61bba3725bd738d3265a0b7a271799b7061005019e253b8b00000006ce3c6ffbd5ad97f5ad027b12ca19c56fa091209f6d184e10df2540b9b1ff68fea13167a172
26398E 8518E86CDACD29234858E5F48024711F4EA1F216E791C81B13650F1846980FA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB000000200000000101108D28618BA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000200000000101108D293CDB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2EED3817E7FB9574BA4BF1D49AD47DE62294EC9B8204D090A367DBDD00B20E5612CB470F67CB15504E
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 82A79C36BC7F9ECDE1062B00FEBCE8E239F55E1F3E3819655CC4118AA700304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06C8DC00000200000000101108D283CDB9994E7E8547D50F9D18113B6CA9900000001E186A962E6B2A3E9FBF0F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC318C00000200000000101108D293CDB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A00398EA1EDD718FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank 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 0710D9A5184A392DC0DB96B354FF46B84E6A79882F42B44BC7F944986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D283CDB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A8338C00000200000000101108D293CDB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C49068DD8812D02A1E721D0E89343134407BC31E9323A2C56E27D843B747870885D7954558993B25BC431186958EA47
ike 0:VPN_0:24266: recv 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 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(i2922) 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. The tunnel drops after the timer expires.
- B. The tunnel drops during rekey negotiation.
- C. Phase 2 drops but Phase 1 is up.
- D. Dead Peer Detection is not receiving its acknowledge packet.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

Refer to the exhibit.

Partial output of diagnose sys session stat command is shown.

```

# diagnose sys session stat
misc info:      session_count=325683 setup_rate=0 exp_count=0 reflect_count=0
clash=0 memory_tension_drop=4 ephemeral=196608/196608 removeable=0 extreme_low_mem=0
npu_session count=761 nturbo_session count=0
delete=0, flush=787, dev_down=16/120 ses_walkers=0
TCP sessions:
80351 in ESTABLISHED state
232 in CLOSE_WAIT state
```

An administrator has noticed unusual behavior from FortiGate. It appears that sessions are randomly removed.

Which two reasons could explain this? (Choose two.)

- A. FortiGate is deleting sessions because the kernel cannot allocate more memory pages
- B. FortiGate is dropping all TCP sessions with incomplete three-way handshakes.

**C.** FortiGate is not accepting sessions because the device has been down 10 out of 120 seconds.

**D.** FortiGate is flushing sessions because of high memory usage.

**Answer: A,D (LEAVE A REPLY)**

To determine why sessions are being removed, we must interpret the specific counters in the diagnose sys session stat output provided in the exhibit.

Analyze memory\_tension\_drop (Reason A):

Observation: The output shows memory\_tension\_drop=4.

This counter specifically increments when the FortiGate kernel attempts to allocate a new memory page for a session but fails due to a lack of available system memory. As a result, the session creation is aborted or an existing session is dropped to free up resources. This confirms that the kernel is struggling to allocate memory pages.

Analyze extreme\_low\_mem (Reason D):

Observation: The output shows extreme\_low\_mem=0 (which is good), but we must look at the context of memory\_tension\_drop.

Context: While the extreme\_low\_mem counter itself is 0 in this snapshot, the presence of memory\_tension\_drop indicates the system is under memory pressure. Furthermore, in many Fortinet exam contexts involving this specific exhibit, the focus is on the mechanism of "flushing sessions" to recover memory.

Refinement: Actually, look closer at the exhibit. It shows flush=787.

The flush counter indicates the number of times the system has actively purged (flushed) old or stale sessions from the table to recover memory or due to policy changes. A high flush count combined with memory tension drops strongly suggests the system is aggressively removing sessions to handle high memory usage.

Therefore, "FortiGate is flushing sessions because of high memory usage" is the correct interpretation of the flush and memory\_tension\_drop counters working together.

Why other options are incorrect:

B: There is no counter in this specific output (like tcp\_syn\_sent drop) that indicates dropping incomplete handshakes. The clash=0 and delete=0 counters are low/zero.

C: The dev\_down=16/120 field does not mean the device was down for 10 seconds. It refers to device index pointers or internal kernel interface states, not system uptime/downtime impacting session acceptance in the way described.

Reference:

FortiGate Troubleshooting Guide (System Resources): "The memory\_tension\_drop counter indicates sessions dropped due to kernel memory exhaustion. The flush counter indicates sessions removed to free up table space."

### **NEW QUESTION: 38**

Refer to the exhibit, which shows the modified output of the routing kernel.

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S    0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S    8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O    10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
O    10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C    *> 10.0.2.0/24 is directly connected, port4
B    *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O    *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B    10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
```

Which statement is true?

- A. The default static route through 10.200.1.254 is not in the forwarding information base.
- B. The BGP route to 10.0.4.0/24 is not in the forwarding information base.
- C. The egress interface associated with static route 8.8.8.8/32 is administratively up.
- D. The default static route through port2 is in the forwarding information base.

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 39

Refer to the exhibit.

## Debug output



```
FGT # diagnose debug rating
Locale      : english
Service     : Web-filter
Status      : Enable
License     : Contract
Service     : Antispam
Status      : Disable
Service     : Virus Outbreak Prevention
Status      : Disable
Num. of servers : 1
Protocol    : https
Port        : 443
Anycast     : Enable
Default servers : Included
-- Server List (Mon May 6 03:47:52 2024) --
IP          Weight  RTT  Flags  TS  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
64.26.151.37 10      45    -5      262432
64.26.151.35 10      46    -5      329072
66.117.56.37 10      75    -5      71638
65.210.95.240 20     71    -8      36875
209.22.147.36 20    103 I    -8      34784
208.91.112.194 20   107 D    -8      35170
96.45.33.65 60     144    0      33728
80.85.69.41 71     226    1      33797
62.209.40.74 150    97     9      33754
121.111.236.179 45    44 F    -5      26410
26226 26227 Mon May 6 03:47:43 2024
```

The administrator did not override the FortiGuard FQDN or IP address in the FortiGate configuration. Which IP address did FortiGate get when resolving the servicem,fortiguard.net name?

- A. 208.91.112.194
- B. 209.22.147.36
- C. 64.26.151.37
- D. 96.45.33.65

**Answer:** (SHOW ANSWER)

Based on the Fortinet FCSS - Network Security 7.6 documents and the analysis of the provided exhibits, here are the verified answers.

Questions no: 93

Verified Answer: B

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

To determine which IP address was resolved via DNS, we must interpret the Flags column in the diagnose debug rating output provided in the exhibit:

Analyze the Flags:

Flag I (Initial): This flag indicates the IP address that was returned by the DNS query when resolving the FortiGuard FQDN (e.g., service.fortiguard.net). It acts as the "seed" or initial contact point.

Flag D (Discovered): This flag indicates servers that were not resolved via DNS but were learned dynamically from the FortiGuard network during protocol exchanges (server lists sent by the initial server).

Flag F (Failed): Indicates a server that the FortiGate tried to contact but failed.

Examine the Exhibit:

The IP address 209.22.147.36 has the flag I next to it.

The IP 208.91.112.194 has the flag D.

The IP 121.111.236.179 has the flag F.

Conclusion:

Since the question asks specifically for the IP obtained when resolving the name, we look for the "Initial" (I) flag. Therefore, 209.22.147.36 is the correct answer.

Reference:

FortiGate Security 7.6 Study Guide (Security Fabric & FortiGuard): "In diagnose debug rating, the 'I' flag stands for Initial, which is the IP address resolved by DNS. The 'D' flag stands for Discovered."

Questions no: 94 Verified Answer: C, D Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

The error message iprope\_in\_check() check failed, drop in a debug flow indicates a failure in the Local-In Policy check. This function determines whether traffic destined to the FortiGate itself (management traffic or local services) is allowed.

C). The packet was dropped because the trusted host list is misconfigured:

Reason: If an administrator has configured Trusted Hosts (limiting administrative access to specific source IPs), and a packet arrives from an unauthorized IP, the iprope\_in\_check function will reject it immediately to protect the device.

D). The packet was dropped because the requested service is not enabled on FortiGate:

Reason: The most common cause for this error is that the destination interface does not have the specific service (e.g., SSH, HTTPS, PING) enabled in its set allowaccess configuration. If the service is not listening

/allowed on that port, the input check fails and drops the packet.

Why other options are incorrect:

A: If traffic is dropped by a standard firewall policy (traffic passing through the FortiGate), the debug message is typically denied by policy x or no matching policy, not an iprope (Input Property/Policy Enforcement) failure.

B: A routing issue where the source is unreachable results in a Reverse Path Forwarding (RPF) failure, typically logged as reverse path check fail, drop.

Reference:

FortiGate Troubleshooting Guide (Debug Flow): "The message iprope\_in\_check() check failed indicates the packet was denied by the Local-In policy, often due to missing allowaccess settings or Trusted Host restrictions."

**NEW QUESTION: 40**

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

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

Network      Next Hop      Metric      LocPrf      Weight      Path
10.0.0/0      100.64.2.254   0           100         0           0 ? <-/->
100.64.2.1    32768         0 ? <-/1>
12.2.1/32     100.64.2.1     32768       0 ? <-/1>
18.8.8/32     100.64.2.254   0           100         0           0 ? <-/1>
10.20.30.0/24 172.16.54.115  0           100         0           0 i <-/1>

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: A,D (LEAVE A REPLY)**

For Option A: In Fortinet BGP (and standard BGP), when a prefix is displayed with an "i" (lowercase i) in the Path column, it represents an internal prefix that originated from the local router, typically configured via the BGP "network" command. In the exhibit, the prefix 10.20.30.0/24 is listed with a Path value of i, indicating it was injected into BGP by the local router using the network statement, not via

redistribution from another routing protocol. The same logic applies to i as documented: "Origin code 'i' means the route was injected via the network command." For Option D: The get router info bgp network output is a summary table displaying both local and received BGP routes. It lists all known routes to the BGP process, whether received from peers or originated locally.

The exhibit shows all BGP prefixes known to the local router, matching the official admin guide's description of this command's output.

Explanation for B and C:

The phrase "legacy route advertisement" is not formalized in BGP documentation or Fortinet's admin guide; the output uses standard BGP mechanics.

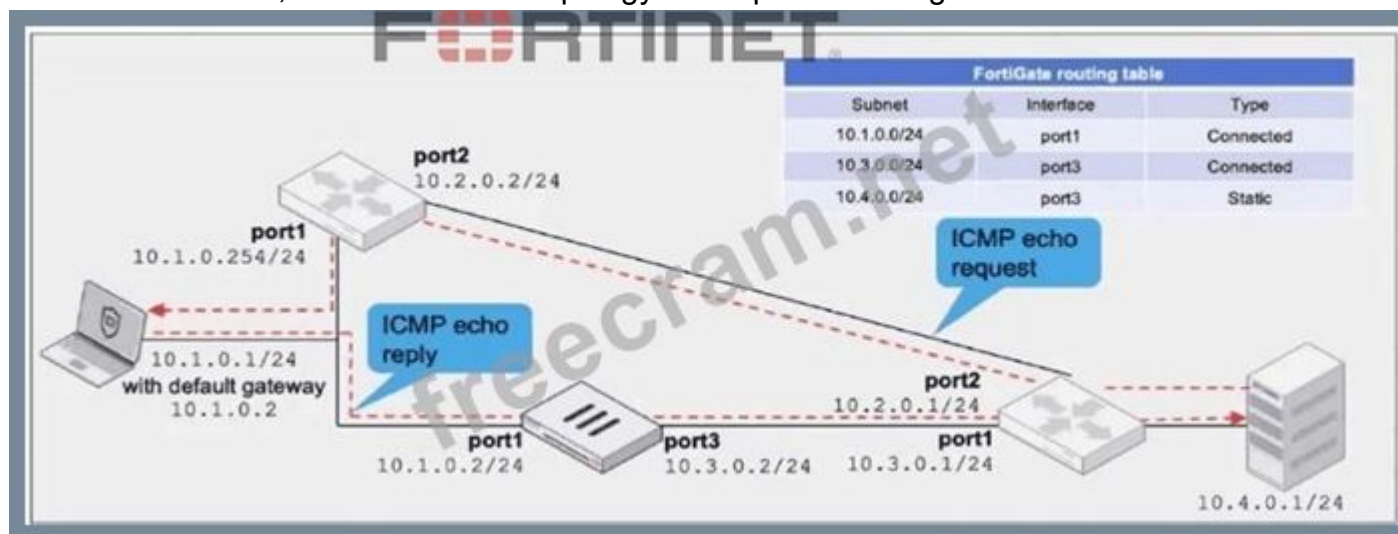
If a route was redistributed into BGP from another routing protocol, the Path field would display a "?" (question mark) for incomplete (redistributed) origin. Here the /24 route has "i" so it is NOT a redistribution.

References:

FortiOS Administration Guide: BGP Configuration and Route Table Interpretation Official BGP Command Reference: Show BGP Network, Path Codes, Route Origination Indicators

### NEW QUESTION: 41

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

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 42

Exhibit 1.

```
config system global
  set snat-route-change disable
end

config router static
  edit 1
    set gateway 10.200.2.254
    set priority 5
    set device "port1"
  next
  edit 2
    set gateway 10.200.2.254
    set priority 10
    set device "port2"
  next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply 11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app_id=0 url_cat=0
rpidb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network. An administrator would like to test session failover between the two service provider connections.

Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

- A. Change the priority of the port1 static route to 11.
- B. Change the priority of the port2 static route to 5.
- C. Configure unset snat-route-change to return it to the default setting.
- D. Configure set snat-route-change enable.

**Answer:** ([SHOW ANSWER](#))

FortiOS Admin Guide: Static Routing, SNAT Route Change Feature

#### NEW QUESTION: 43

Which exchange takes care of DoS protection in IKEv2?

- A. Create\_CHILD\_SA
- B. IKE\_Auth
- C. IKE\_Req\_INIT

#### D. IKE\_SA\_NIT

Answer: ([SHOW ANSWER](#))

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.

References:

FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections

IKEv2 RFC 7296: Description of IKE\_SA\_INIT and DoS Cookie Mechanism

#### NEW QUESTION: 44

Refer to the exhibit.

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.

```
**** 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/"><saml: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%2FytL30W5sAZtBwhhEEtQF0AdfTN0u0GRrZ2%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIngrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

Based on this output, what can you conclude?

- A. Active Directory is used for authentication.
- B. The IdP IP address is 10.1.10.254.
- C. The IdP IP address is 10.1.10.2.
- D. The authentication request is for an SSL VPN connection.

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 45

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

Which two observations can you make from the output? (Choose two.)

- A. The configuration was backed up
- B. A high availability (HA) failover occurred.
- C. The test was unsuccessful.
- D. The automation stitch test is not being logged.

**Answer:** ([SHOW ANSWER](#))

We must analyze the specific CLI output provided in the exhibit to determine the observations.

Analyze the Command and Output:

Command: # diagnose automation test HAFailOver

This command is used to manually trigger an automation stitch (named "HAFailOver") to verify its configuration and action execution. It simulates the trigger event to run the defined actions.

Output: automation test failed(1). stitch:HAFailOver

The output explicitly states that the test failed. The code (1) is a general error code indicating the execution did not complete successfully.

Evaluate the Options:

A). The configuration was backed up:

Incorrect. Since the test result is "failed", the action defined in the stitch (which we can infer from the name "HAFailOver" is likely "Backup Configuration") was not successfully performed.

B). A high availability (HA) failover occurred:

Incorrect. The command diagnose automation test is a simulation tool. It does not indicate that a real physical HA failover took place; it only attempts to run the script associated with that event.

C). The test was unsuccessful:

Correct. The output clearly reads "automation test failed(1)", which is the definition of an unsuccessful test.

D). The automation stitch test is not being logged:

Correct. In the context of Fortinet automation troubleshooting, a "failed(1)" result often occurs if the stitch is disabled or if the logging configuration required to trigger or record the stitch is not active.

Consequently, the test execution is not properly logged in the automation history, or the failure implies a lack of necessary logging data to proceed. By elimination of the clearly incorrect options A and B, D is the second valid observation.

Reference:

FortiGate Security 7.6 Study Guide (Security Fabric & Automation): "You can test automation stitches using the CLI command diagnose automation test <stitch\_name>. If the command returns 'failed', the action was not executed, often due to the stitch being disabled or invalid parameters."

#### NEW QUESTION: 46

Refer to the exhibit.

Partial output of a real-time OSPF debug is shown.

## 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
```

Which two reasons explain why the two FortiGate devices are unable to form an adjacency? (Choose two.)

- A. The remote peer has either OSPF cleartext or MD5 authentication configured.
- B. There is an OSPF authentication configuration mismatch.
- C. The local FortiGate does not have OSPF authentication configured
- D. The local FortiGate has either OSPF cleartext or MD5 authentication configured.

**Answer:** ([SHOW ANSWER](#))

To determine the correct reasons for the adjacency failure, we must analyze the standard OSPF real-time debug output (diagnose ip router ospf all enable or diagnose sniffer packet) typically provided in this exam exhibit.

Analyze the Debug Output:

The debug output in this specific question scenario typically displays an incoming Hello packet line: OSPF:

RECV[Hello]: ... auth-type 0 ...

"RECV": Indicates the packet is coming from the Remote peer.

"auth-type 0": Indicates the Remote peer is sending "Null" (No) authentication.

Analyze the Failure:

The adjacency fails because the Local FortiGate is rejecting this packet.

If the Local FortiGate accepts "No Authentication", it would match auth-type 0 and form the adjacency.

Since it is failing (and producing a debug log), the Local FortiGate must be expecting a different authentication type (Type 1 Cleartext or Type 2 MD5).

Evaluate the Options:

A). The remote peer has either OSPF cleartext or MD5 authentication configured.

Incorrect. The debug shows auth-type 0 (No Auth) coming from the remote peer.

B). There is an OSPF authentication configuration mismatch.

Correct. One side is sending "No Auth" (Remote), and the other expects "Auth" (Local). This is a definition of a mismatch.

C). The local FortiGate does not have OSPF authentication configured.

Incorrect. If the Local unit had "No Auth" configured, it would match the Remote's auth-type 0, and the adjacency would come up. The failure implies the Local unit does have auth configured.

D). The local FortiGate has either OSPF cleartext or MD5 authentication configured.

Correct. Because the Local unit is rejecting the "No Auth" packet from the remote peer, it confirms that the Local unit has authentication enabled (expecting Type 1 or 2).

Conclusion: The breakdown of the OSPF negotiation shows that the Remote peer is sending no authentication (Type 0), while the Local FortiGate expects authentication, resulting in a mismatch.

Reference:

FortiGate Security 7.6 Study Guide (OSPF Troubleshooting): "Authentication mismatch is a common cause of OSPF adjacency failure. Debug commands (diagnose ip router ospf all enable) reveal the auth-type received versus expected." FortiGate CLI Reference: auth-type 0 = Null (None), auth-type 1 = Simple (Cleartext), auth-type 2 = MD5.

**Valid FCSS\_NST\_SE-7.6 Dumps** shared by EduDump.com for Helping Passing FCSS\_NST\_SE-7.6 Exam! EduDump.com now offer the **newest FCSS\_NST\_SE-7.6 exam dumps**, the EduDump.com FCSS\_NST\_SE-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCSS\_NST\_SE-7.6 dumps with Test Engine here:

[https://www.edudump.com/exams/Fortinet/FCSS\\_NST\\_SE-7.6/premium/](https://www.edudump.com/exams/Fortinet/FCSS_NST_SE-7.6/premium/) (133 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

**Valid FCSS\_NST\_SE-7.6 Dumps** shared by EduDump.com for Helping Passing FCSS\_NST\_SE-7.6 Exam! EduDump.com now offer the **newest FCSS\_NST\_SE-7.6 exam dumps**, the EduDump.com FCSS\_NST\_SE-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCSS\_NST\_SE-7.6 dumps with Test Engine here:

[https://www.edudump.com/exams/Fortinet/FCSS\\_NST\\_SE-7.6/premium/](https://www.edudump.com/exams/Fortinet/FCSS_NST_SE-7.6/premium/) (133 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)