Product Questions: 99
Version: 6.4

Question: 1

Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.

Which action will FortiGate take when using the default settings for SSL certificate inspection?
A. FortiGate uses the SNI from the user's web browser.
B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
C. FortiGate uses the first entry listed in the SAN field in the server certificate.
D. FortiGate uses the CN information from the Subject field in the server certificate.

Answer: D

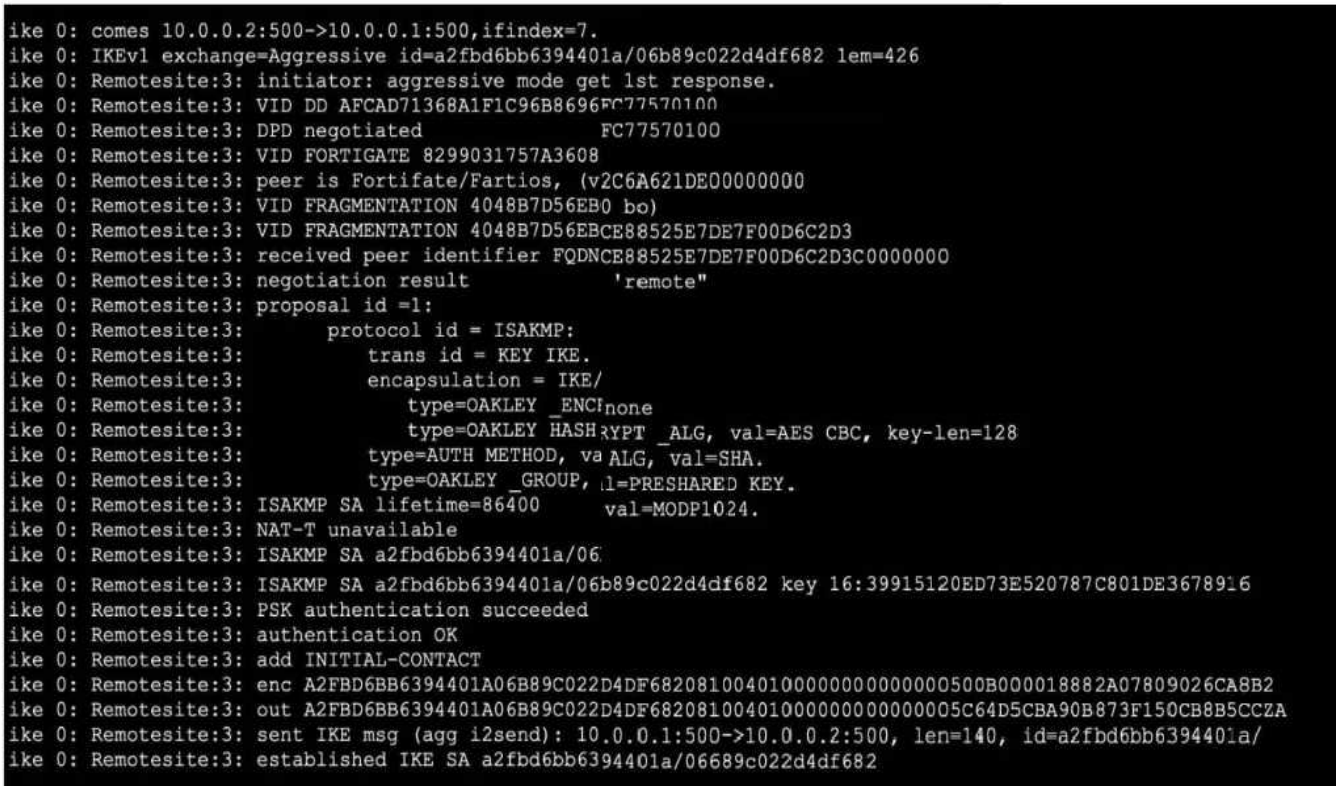
Explanation:

When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, 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.
Reference:

FortiGate 7.6.4 Administration Guide: Certificate Inspection
SSL/SSH Inspection Profile Configuration

Question: 2

Exhibit.



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: C,D

Explanation:

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.

Reference:

FortiOS 7.6.4 Administration Guide: IPsec VPN and Debugging VPNs

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

Question: 3

Exhibit.

```
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  1 03:47:52 2023) -=-

IP                                     Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                               10     45          -5              262432         0        846 Mon May  1 03:47:43 2023
64.26.151.35                               10     46          -5              329072         0       6806 Mon May  1 03:47:43 2023
66.117.56.37                               10     75          -5               71638         0        275 Mon May  1 03:47:43 2023
65.210.95.240                              20     71          -8               36875         0         92 Mon May  1 03:47:43 2023
209.22.147.36                              20     103 DI      -8               34784         0       1070 Mon May  1 03:47:43 2023
208.91.112.194                             20     107 D       -8               35170         0       1533 Mon May  1 03:47:43 2023
                                                                0               33728         0        120 Mon May  1 03:47:43 2023
                                                                1               33797         0        192 Mon May  1 03:47:43 2023
                                                                9               33754         0        145 Mon May  1 03:47:43 2023
                                                               -5               26410         26226  26227 Mon May  1 03:47:43 2023
```

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

What can you conclude about the debug output in this scenario?

A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.

C. FortiGate used 64.26.151.37 as the initial server to validate its contract.

D. Servers with a negative TZ value are less preferred for rating requests.

Answer: C

Explanation:

The exhibit displays the output from the diagnose debug rating command on a FortiGate device. This command is used to display information about FortiGuard Web Filtering or other security-related queries performed by FortiGate to FortiGuard servers. Official Fortinet documentation outlines the meaning of each field in the server list. The FortiGate maintains a list of available FortiGuard servers, selecting the optimal server based on factors such as weight, round-trip time (RTT), and regional settings.

The very first entry in the server list after "Server List" is the server FortiGate initially uses, prioritized by factors such as proximity and RTT. Here, 64.26.151.37 is listed first, and the FortiGuard-requests value confirms that this server handled the highest number of requests.

The IPs, weights, and lost/failed counters are monitored for server performance and selection over time. FortiGate's default operational logic is to try the first entry for contract validation and use the next in the list if the first is unavailable or has high latency or packet loss.

There is no direct correlation between the Weight and the number of FortiGuard-requests. The servers with higher or lower weights may still handle different request volumes based on availability and performance.

The TZ (time zone) value's sign (positive or negative) does not affect server preference; it is informational, showing the server's location relative to UTC, not a rating metric.

DNS query results for FortiGuard servers are not shown here, and the provided servers are not returned in DNS query order.

This command and interpretation are detailed in the FortiOS Administration Guide's section describing FortiGuard server selection and contract validation processes.

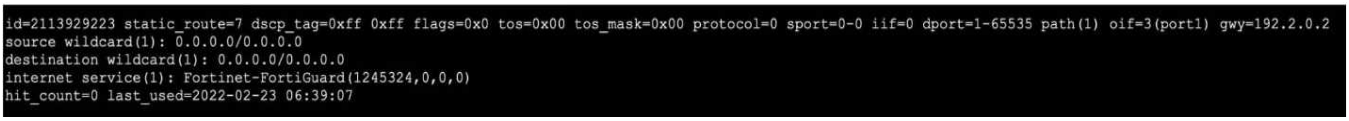
Reference:

FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging

Official Technical Notes on diagnose debug rating output structure

Question: 4

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



Which type of policy route does the output show?

A. An ISDB route

B. A regular policy route

C. A regular policy route, which is associated with an active static route in the FIB

D. An SD-WAN rule

Answer: A

Explanation:

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

Question: 5

Exhibit.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-iD6 ::
    set proxv-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dons-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.

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

What must the administrator do to fix the issue?

A. Disable webfilter-force-off.

B. Increase webfilter-timeout.

C. Enable fortiguard-anycast.

D. Change protocol to TCP.

Answer: A

Explanation:

The exhibit shows a FortiGate configuration under config system fortiguard related to web filtering and FortiGuard options. There is a line:
set webfilter-force-off enable
According to official Fortinet documentation, the "webfilter-force-off" option, when enabled, causes the FortiGate to bypass web filtering for all traffic—even if a web filter profile is applied to a policy. This override is typically used for troubleshooting or performance reasons and is documented as an explicit bypass feature.
If an administrator wants to enforce web filtering inspection, this setting must be disabled.
The correct way to restore web filtering functionality is to run:
set webfilter-force-off disable
Once done, traffic passing through policies with web filter profiles will be inspected and filtered as per configuration. Other settings such as timeout or cache TTL do not bypass web filtering; they only affect operational nuances.
Reference:
FortiOS Administration Guide: Web Filtering, FortiGuard Options, “webfilter-force-off” CLI

Question: 6

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: D

Explanation:

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

Question: 7

Exhibit 1.

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

```
config router static
    edit 1
        set gateway 10.200.1.254
        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
orgin->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=0 url_cat=0
rpdb_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 lest 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: A,D

Explanation:

FortiOS Admin Guide: Static Routing, SNAT Route Change Feature

Question: 8

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

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

  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2

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

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

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

A. The interlace is part of the OSPF backbone area.

B. There are a total of five OSPF routers attached to the vorz4 network segment

C. One of the neighbors has a router ID of 0.0.0.4.

D. In the network connected to port4, two OSPF routers are down.

Answer: A,B

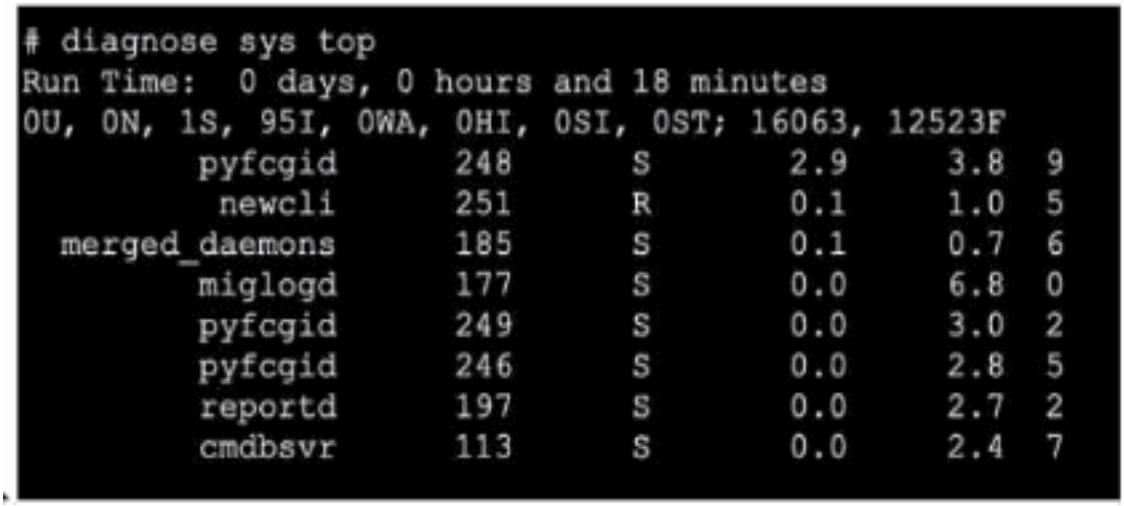
Explanation:

Reference:

FortiOS Admin Guide: OSPF, Debug Outputs

Question: 9

Refer to the exhibit.



Which three pieces of information does the diagnose sys top command provide? (Choose three.)

A. The miglogd daemon is running on CPU core ID 0.

B. The diagnose sys top command has been running for 18 minutes.

C. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.

D. The cmdbsvr process is occupying 2.4% of the total user memory space.

E. If the neweli daemon continues to be in the R state, it will need to be manually restarted.

Answer: A,C,D

Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-diagnose-sys-top-CLI-command/ta-p/190238

Question: 10

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

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

Network          Next Hop            Metric     LocPrf Weight RouteTag Path
.0.0.0/0         100.64.2.254    0              100      0        0 ? <-/->
                 100.64.2.1                          32768        0 ? <-/1>
.2.2.1/32        100.64.2.1                          32768        0 ? <-/1>
.8.8.8/32        100.64.2.254    0              100      0        0 ? <-/1>
0.20.30.0/24     172.16.54.115   0              100      0        0 i <-/1>

l 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

Explanation:

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.

Reference:

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

Question: 11

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

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

Answer: A,C

Explanation:

Question: 12

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

```
get router info bgp summary

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

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

Total number of neighbors 2
```

Which two statements are true? (Choose two.)
A. The local ForliGate has received one prefix from BGP neighbor 100.64.1.254.
B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
C. The local FortiGate has received 18 packets from a BGP neighbor.
D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: A,C

Explanation:

The get router info bgp summary output lists BGP neighbor status:

Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.

Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.

The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B.

There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect.

Reference:

FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters

Question: 13

Which exchange lakes care of DoS protection in IKEv2?

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

Answer: C

Explanation:

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.
Reference:
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections

IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

Question: 14

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

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

What two conclusions can you draw from the output? (Choose two.)
A. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on.
B. The logon event can be seen on the collector agent installed on Windows.
C. FSSO is using DC agent mode to detect logon events.
D. FSSO is using agentless polling mode to detect logon events.

Answer: A,D

Explanation:

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349

From the snippet we can see that FortiGate (via the fssod daemon) is directly detecting the user logon rather than relying on a separate “collector” or “DC agent.” This indicates agentless polling—FortiGate polls the DC’s event logs over TCP 445 to discover logons. So: - FSSO is using agentless polling mode to detect logon events - In agentless mode, FortiGate will periodically poll the same IP (the DC) on port 445 to see if the user is still logged on

Question: 15

An administrator wants to capture encrypted phase 2 traffic between two FotiGate 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 'lp proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'ah'

Answer: B

Explanation:

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

Question: 16

Refer to the exhibits.

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

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

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

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

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

Answer: B

Explanation:

The 8.8.8.8/32 route is visible in the OSPF database on FGT-B but not installed into the routing table—the most likely explanation is that FGT-B is filtering it from being installed.

Question: 17

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

```
# get router info bgp summary

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

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

Total number of neighbors 3
```

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

Answer: D

Explanation:

The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show "Idle," "Active," or "Connect," but instead shows "Established," "Up," or related

counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.
The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.
Reference:
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

Question: 18

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

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

Answer: B,C

Explanation:

Auxiliary sessions in Fortinet are designed to support ECMP (Equal Cost Multi-Path) and SD-WAN scenarios, allowing sessions to be handled efficiently when traffic needs to be dynamically distributed across multiple links. With the auxiliary session setting enabled, FortiGate creates additional session table entries for each possible path in ECMP or SD-WAN—meaning that if the routing path changes (such as a link failover), a new session can be immediately activated and offloaded to the NP6 network processor for acceleration, ensuring minimal disruption. This greatly benefits high-throughput deployments.
Official documentation specifies that when auxiliary sessions are enabled, FortiGate doesn’t just rely on dynamically creating new sessions after a routing event, it proactively creates sessions for all potential paths. This means that in the event of a route change, two sessions exist and the traffic is quickly re-routed and offloaded, maximizing performance and reliability. Without this feature, multiple paths cannot be efficiently offloaded, and routing changes trigger a single session update, reducing failover performance.
Reference: