



Vendor: Fortinet

Exam Code: FCSS_NST_SE-7.4

Exam Name: FCSS - Network Security 7.4 Support
Engineer

Version: DEMO

QUESTION 1

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

```
get router info bgp summary

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

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

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

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

Answer: AC

QUESTION 2

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: C

QUESTION 3

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

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

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

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

Answer: AD

QUESTION 4

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: B

QUESTION 5

Refer to the exhibits. 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?

```
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 800000002  3106   0002 E2 8.8.8.8/32    0
```

- A. A better 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-B is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

QUESTION 6

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 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: D

QUESTION 7

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

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

Answer: BC

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



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



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14