

Fortinet

Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer



NEW QUESTION 1

Exhibit.

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

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

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

Answer: AD

NEW QUESTION 2

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 interface is part of the OSPF backbone area.
- B. There are a total of five OSPF routers attached to the port4 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: AD

NEW QUESTION 3

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
[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

NEW QUESTION 4

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

NEW QUESTION 5

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

NEW 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

NEW QUESTION 7

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

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

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

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

Answer: D

NEW QUESTION 8

Exhibit.

Edit Web Filter Profile

Bandwidth Consuming 6

Freeware and Software Downloads	<div><div></div></div> Allow
File Sharing and Storage	<div><div></div></div> Block
30% 93	

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
*dropbox.com	Wildcard	<div><div></div></div> Allow	<div><div></div></div> Enable
1			

Block malicious URLs discovered by FortiSandbox

Content Filter

+ Create New

Edit

Delete

Pattern Type ⇅	Pattern ⇅	Language ⇅	Action ⇅	Status ⇅
Wildcard	*dropbox*	Western	<div><div></div></div> Exempt	<div><div></div></div> Enable

NEW QUESTION 9

Which statement about parallel path processing is correct (PPP)?

- A. PPP chooses from a group of parallel options to identify the optimal path for processing a packet.
- B. Only FortiGate hardware configurations affect the path that a packet takes.
- C. PPP does not apply to packets that are part of an already established session.
- D. Software configuration has no impact on PPP.

Answer: A

NEW QUESTION 10

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

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

Answer: D

NEW QUESTION 10

Which statement about protocol options is true?

- A. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
- B. Protocol options give administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
- C. Protocol options allow administrators to configure the Any setting for all enabled protocols, which provides the most efficient use of system resources.
- D. Protocol options allow administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

Answer: D

NEW QUESTION 13

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

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

Answer: BC

NEW QUESTION 18

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: BC

NEW QUESTION 22

Exhibit.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 lem=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 FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result 'remote"
ike 0: Remotesite:3: proposal id =1:
ike 0: Remotesite:3: protocol id = ISAKMP:
ike 0: Remotesite:3: trans id = KEY IKE.
ike 0: Remotesite:3: encapsulation = IKE/
ike 0: Remotesite:3: type=OAKLEY_ENCI none
ike 0: Remotesite:3: type=OAKLEY_HASHRYPT_ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3: type=AUTH METHOD, va ALG, val=SHA.
ike 0: Remotesite:3: type=OAKLEY_GROUP, l=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400 val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CCZA
ike 0: Remotesite:3: sent IKE msg (agg i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06689c022d4df682
```

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

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

Answer: CD

NEW QUESTION 25

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

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

FortiGate # get router info routing-table all

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

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

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

Answer: D

NEW QUESTION 28

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

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

Which type of policy route does the output show?

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

Answer: A

NEW QUESTION 29

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

FCSS_NST_SE-7.4 Practice Exam Features:

- * FCSS_NST_SE-7.4 Questions and Answers Updated Frequently
- * FCSS_NST_SE-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_NST_SE-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_NST_SE-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_NST_SE-7.4 Practice Test Here](#)