

# Fortinet

## Exam Questions FCSS\_NST\_SE-7.4

FCSS - Network Security 7.4 Support Engineer



### NEW QUESTION 1

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
```

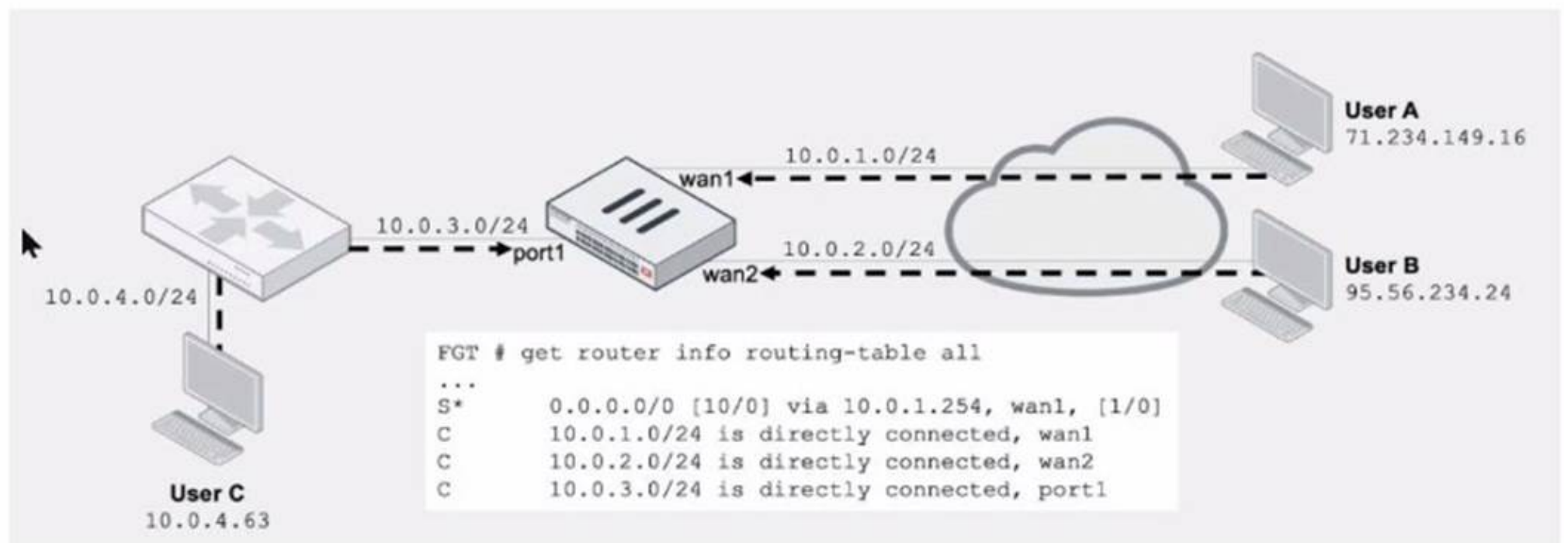
Which two statements about the output are true? (Choose two.)

- 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 2

Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three.)

- A. Strict RPF is enabled by default.
- B. User B: Fai
- C. There is no route to 95.56.234.24 using wan2 in the routing table.
- D. User A: Pas
- E. The default static route through wan1 passes the RPF check regardless of the source IP address.
- F. User B: Pas
- G. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
- H. User C: Fai
- I. There is no route to 10.0.4.63 using port1 in the routing table.

**Answer: BDE**

### NEW QUESTION 3

Exhibit.

Name

Remote

Comments

Comments

0/255

Network

IP Version

IPv4

IPv6

Remote Gateway

Static IP Address

IP Address

10.0.10.1

Interface

port1

Local Gateway

Mode Config

NAT Traversal

Enable

Disable

Forced

Keepalive Frequency

10

Dead Peer Detection

Disable

On Idle

On Demand

Refer to the exhibit, which contains a screenshot of some phase 1 settings.

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

However, the IKE real-time debug does not show any output. Why?

- A. The administrator must also run the command `diagnose debug enable`.
- B. The debug shows only error message
- C. If there is no output, then the phase 1 and phase 2 configurations match.
- D. The log-filter setting is incorrect
- E. The VPN traffic does not match this filter.
- F. Replace `diagnose debug application ike -1` with `diagnose debug application ipsec -1`.

**Answer:** A

#### 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\_INIT

**Answer:** C

#### NEW QUESTION 5

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
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=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 unsetsnat-route-change to return it to the default setting.
- D. Configure setsnat-route-change enable.

Answer: AD

#### NEW QUESTION 6

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 7

Exhibit.

Edit Web Filter Profile

Bandwidth Consuming 6

Freeware and Software Downloads	 Allow
File Sharing and Storage	 Block






30% 93

Allow users to override blocked categories

Static URL Filter





Block invalid URLs

URL Filter

<div>+ Create New</div>	<div> Edit</div>	<div> Delete</div>	<div>Search</div>	<div></div>
URL	Type	Action	Status	
*dropbox.com	Wildcard	 Allow	 Enable	
1				

Block malicious URLs discovered by FortiSandbox

Content Filter

<div>+ Create New</div>	<div> Edit</div>	<div> Delete</div>		
Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	 Exempt	 Enable

Refer to the exhibit, which shows a partial web filter profile configuration.  
 Which action does FortiGate take if a user attempts to access www. dropbox. com, which is categorized as File Sharing and Storage?

A. FortiGate allows the connection, based on the URL Filter configuration.  
 B. FortiGate blocks the connection as an invalid URL.  
 C. FortiGate exempts the connection, based on the Web Content Filter configuration.  
 D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Answer: D



**NEW QUESTION 8**

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 9**

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 10**

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/Fortios, (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_HASH_2YPT_ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3: type=AUTH METHOD, val=ALG, val=SHA.
ike 0: Remotesite:3: type=OAKLEY_GROUP, val=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/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 A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07809026C8B2
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/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: CD**

**NEW QUESTION 10**

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 13

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:** D

#### NEW QUESTION 16

In IKEv2, which exchange establishes the first CHILD\_SA?

- A. IKE\_SA\_INIT
- B. INFORMATIONAL
- C. CREATE\_CHILD\_SA
- D. IKE\_Auth

**Answer:** C

#### NEW QUESTION 18

.....



## 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](#)**