FCSS_NST_SE-7.4 Dumps

FCSS - Network Security 7.4 Support Engineer

https://www.certleader.com/FCSS_NST_SE-7.4-dumps.html

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 ofa 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: AD

NEW QUESTION 3
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
```
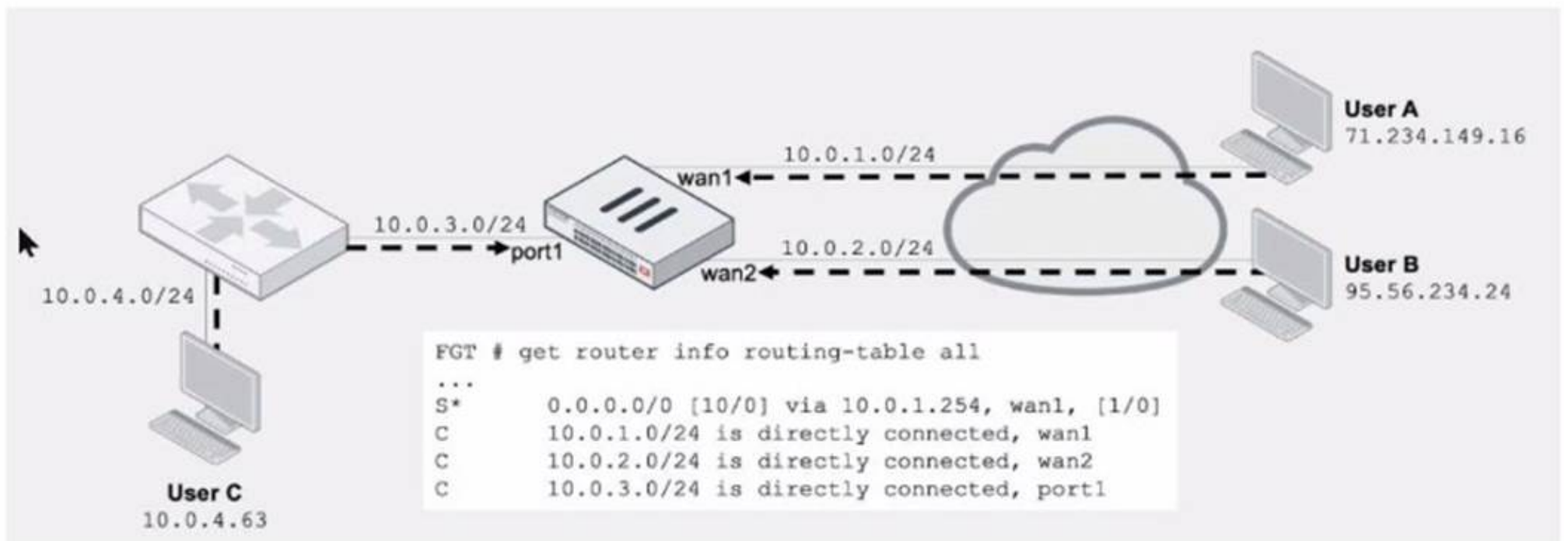
An administrator Is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT- B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

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

NEW QUESTION 4
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 touting table.

Answer: BDE

NEW QUESTION 5
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 Itom 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 6
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: B

NEW QUESTION 7
Exhibit.

```
|.. name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
... failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

Refer to the exhibit, which shows two entries that were generated in theFSSO collectoragent logs.
What three conclusions can you draw from these log entries? {Choose three.)

A. Remote registry is not running on the workstation.
B. The user's status shows as "not verified" in the collector agent.
C. DNS resolution is unable to resolve the workstation name.
D. The FortiGate firmware version is not compatible with that of the collector agent.
E. A firewall is blocking traffic to port 139 and 445.

Answer: ABE

NEW QUESTION 8
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: AC

NEW QUESTION 9
Which statement about IKEv2 is true?

A. Both IKEv1and IKEv2 share the feature of asymmetric authentication.
B. IKEv1and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1and IKEv2 share the concept of phase1and phase2.

Answer: B

NEW QUESTION 10
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 port! 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 10
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

NEW QUESTION 13
Refer to the exhibit, which shows a truncated 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_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: BD

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 authed 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)
pos/(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
rpdb_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 Iwo.)

A. The TCP session has been successfully established.
B. The session was initiated from an authenticated user.
C. The session is being inspected using flow inspection.
D. The session is being offloaded.

Answer: AB

NEW QUESTION 22
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 enable
C. ECMP traffic is accelerated to the NP6 processor.
D. With the auxiliary session setting enable
E. Iwo sessions are created in case of routing change.
F. With the auxiliary session setting disabled, for each traffic pat
G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 24
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 Fortifate/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 HASH RYPT _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 A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF682081004010000000000000C5C64D5CBA90B873F150CB8B5CCZA
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 26
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

NEW QUESTION 31
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 policy route misconfiguration.
B. Packet was dropped because of traffic shaping.
C. Trusted host list misconfiguration.
D. VIP or IP pool misconfiguration.

Answer: CD

NEW QUESTION 34
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_NST_SE-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_NST_SE-7.4-dumps.html