Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
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 2
Refer to the exhibit, which shows the output of diagnose sys session list.

Diagnose output

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 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
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/if ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

A. The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.
B. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.
C. The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.
D. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

Answer: B

NEW QUESTION 3
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:
```

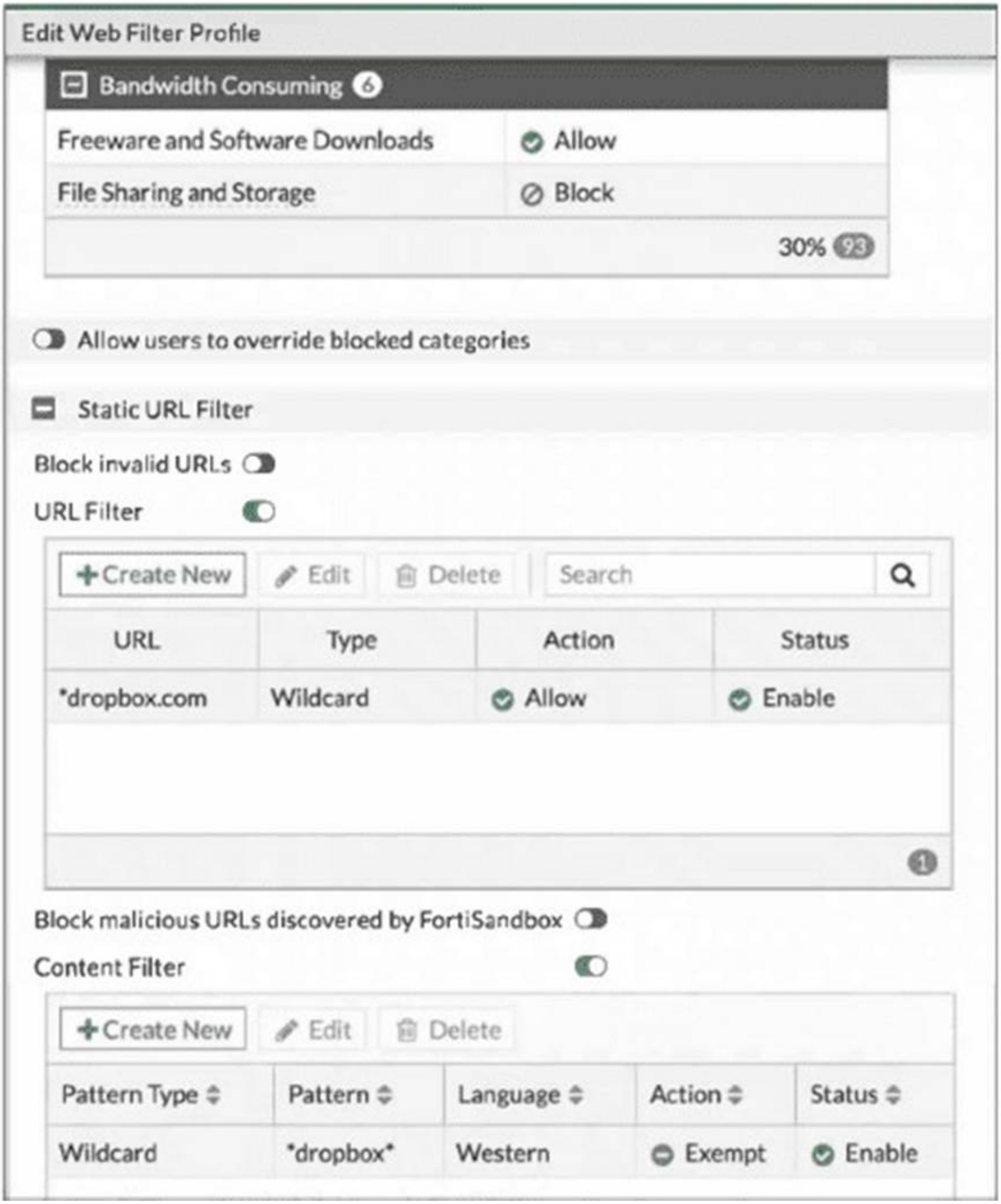
Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.
An administrator would like to lest session failover between the two service provider connections.
Which two changes must the administrator make to force this 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 unset snat-route-change to return it to the default setting.
D. Configure set snat-route-change enable.

Answer: AD

NEW QUESTION 4
Refer to the exhibit, which shows a partial web filter profile configuration.

Web filter profile



The URL www.dropbox.com is categorized as File Sharing and Storage.
Which action does FortiGate take if a user attempts to access www.dropbox.com?

A. FortiGate blocks the connection as an invalid URL.
B. Based on the URL Filter configuration, FortiGate allows the connection.
C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.
D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

Answer: B

NEW QUESTION 5
Refer to the exhibit, which shows the partial output of a real-time OSPF debug.

Real-time OSPF debug output

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF: ----------------------------------------------------
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|-|-|-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Why are the two FortiGate devices unable to form an adjacency?

A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
C. One FortiGate device is configured to require authentication, while the other is not.
D. The passwords on the FortiGate devices do not match.

Answer: C

NEW QUESTION 6
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 7
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 8
Refer to the exhibit, which shows a partial output of the real-time LDAP debug.

```
# fnbamd_fsm.c[1274] handle_req-Rcvd auth req 6750221 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=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 6750221
fnbamd_ldap.c[275] get_all_dn-Found no DN
fnbamd_ldap.c[298] start_next_dn_bind-No more DN left
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending result 1 for req 6750221
```

What two actions can the administrator take to resolve this issue? (Choose two.)

A. Ensure the user logs in using 'John Smith' not 'jsmith'.
B. Ensure the user is providing the correct user credentials.
C. Ensure the user is a member of at least one AD group to ensure step 4 of the LDAP authentication process is successful.
D. Ensure the account is active.

Answer: BD

NEW QUESTION 9
Which two statements about conserve mode are true? (Choose two.)

A. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
B. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
C. FortiGate exits conserve mode when the system memory goes below the configured green threshold.
D. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.

Answer: BC

NEW QUESTION 10
Which statement about parallel path processing is correct (PPP)?

A. PPP chooses from a group of parallel options lo identity the optimal path tor 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

Explanation:
Parallel Path Processing (PPP) in FortiOS refers to the system??s ability to evaluate and select among multiple processing paths—often involving dedicated network processors, content processors, or CPU-based workflows—to optimally process packets. The official documentation highlights that the PPP engine dynamically selects which hardware or software path to use for each session based on session characteristics, policy configuration, and traffic type. This dynamic selection results in optimal throughput and resource utilization.
The document specifies that PPP assesses several processing paths in parallel, using decision logic to determine whether a session should be offloaded to specialist hardware (like NP6, CP9, etc.) or stay in the CPU path, ensuring that each packet is handled by the most efficient available method under current load and policy. Hardware and software configurations both influence this outcome, but it is the PPP engine's decision-making that defines the optimal path per session.
[References:, Fortinet FortiGate Handbook: Parallel Path Processing, Fortinet FortiOS Technical Documentation: Packet Flow and Path Selection,]

NEW QUESTION 10
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 the FSSO collector agent 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 13
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)
A. You must authorize the downstream FortiGate on the root FortiGate.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way.
D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
E. Ensure the port for Neighbor Discovery has been changed.

A.

Answer: ACD

NEW QUESTION 16
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 lo 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: B

Explanation:
The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, thehook=post dir=org act=snatshows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a TCP/UDP port). The reply direction,hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.
FortiOS Administration Guide: Session Table, NAT, and Route Interaction
Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION 21
Refer to the exhibit, which shows the output of the command get router info bgp neighbors 100.64.2.254 advertised-routes.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1           xxx       0        0          100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP state of the two BGP participants is OpenConfirm.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Answer: D

NEW QUESTION 25
Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

```
config system interface
    edit "port1"
        set preserve-session-route enable
    next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state=log may_dirty npu f00 route_preserve
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0
```

What happens to the session information if a routing change occurs that affects this session?
A. Only the interface and gateway information for dev=7 will be removed.
B. The session information will not change unless the current route has been removed from the routing table.
C. The session will be flagged as dirty but no route lookups will be performed.
D. Sessions involving port7 or port19 will not have their routing information flushed.

A.

Answer: B

NEW QUESTION 27
Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Which statement is true?
A. The egress interface associated with static route 8.8.8.8/32 is administratively up.

B. The default static route through 10.200.1.254 is not in the forwarding information base.
C. The default static route through port2 is in the forwarding information base.
D. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

A.

Answer: D

NEW QUESTION 32
Refer to the exhibits.

Exhibit 1

```
FGT-A # get router info bgp summary
...

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4      65110    2500    2552        5    0    0 1d11h33m          0
```

Exhibit 2

```
FGT-B # show router bgp

     config network
         edit 1
             set prefix 172.16.0.0 255.255.0.0
         next
     end
```

Exhibit 3

```
FGT-B # diagnose ip address  list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.
Which two actions can the administrator take to fix this problem? (Choose two.)

A. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.
B. Manually add the BGP route on FGT-A.
C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
D. Use the set network-import-check disable command.

Answer: AD

NEW QUESTION 33
In IKEv2, which exchange establishes the first CHILD_SA?

A. IKE_SA_INIT
B. INFORMATIONAL
C. CREATE_CHILD_SA
D. IKE_Auth

Answer: A

Explanation:
According to RFC 7296 (IKEv2) and Fortinet's official documentation, theIKE_SA_INIT exchangeis responsible for negotiating cryptographic parameters, performing the initial Diffie-Hellman exchange, and implementing the cookie challenge mechanism for DoS protection. When the responder suspects a DoS attack (such as mass requests by the same source), it includes a cookie in the IKE_SA_INIT response. The initiator must return the cookie in its next request to prove that it truly exists at the IP address it claims, thereby mitigating resource exhaustion attacks.
This two-step exchange ensures the responder only allocates resources after successful proof of address, aligning with best security practices. Fortinet documentation confirms that this process occurs strictly in the IKE_SA_INIT phase, not in subsequent IKE_Auth or CHILD_SA exchanges.
[References:, RFC 7296: IKEv2, Section 2.6, ??Denial of Service Protection??, Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism, , ,]

NEW QUESTION 37
Refer to the exhibit, which shows a partial output from the get router info routing-table database command.

```
# get router info routing-table database
---omitted---

Routing table for VRF=0
S           0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S           0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive, [50/0]
---omitted---
```

The administrator wants to configure a default static route for port3 and assign a distance of 50 and a priority of 0.
What will happen to the port1 and port2 default static routes after the port3 default static route is created?

A. The port2 default static route will be injected into the forwarding information base (FIB).
B. The port1 default static route will be injected into the FIB.
C. Neither of the routes shown in the output will be injected into the FIB.
D. Both default static routes shown in the output will be injected into the FIB.

Answer: A

NEW QUESTION 40
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.
[References:, , FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging, , Official Technical Notes on diagnose debug rating output structure]

NEW QUESTION 43

Refer to the exhibit showing a debug output.

```
# diagnose debug application authd 8256
# diagnose debug enable
....
[fsae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 disconnect_server_only
[FSSO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
....
```

An administrator deployed FSSO in DC Agent Mode but FSSO is failing on FortiGate. Pinging FortiGate from where the collector agent is deployed is successful.
The administrator then produces the debug output shown in the exhibit.
What could be causing this error message?

A. The TCP port 445 is blocked between FortiGate and collector agent.
B. The collector agent preshared password is mismatched.
C. The FortiGate cannot resolve the active directory server name.
D. The FortiGate and the collector agent are using different TCP ports.

Answer: D

NEW QUESTION 45
Refer to the exhibit, which shows the omitted output of a session table entry.

```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Which two statements are true? (Choose two.)

A. The traffic has been tagged for VLAN 0000.
B. NP7 is handling offloading of this session.
C. The traffic matches Policy ID 1.
D. The session has been offloaded.

Answer: BD

NEW QUESTION 46
Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

```
...
packet_de_duplication     0      0    128    30    1 : tunables  252  126    0 : slabdata      0      0      0
ip6_nat_record            0      0    128    30    1 : tunables  252  126    0 : slabdata      0      0      0
tcp6_session              0      0   1536     5    2 : tunables   60   30    0 : slabdata      0      0      0
ip6_session               0      0   1300     3    1 : tunables   60   30    0 : slabdata      0      0      0
ip_nat_record             0      0     64    59    1 : tunables  252  126    0 : slabdata      0      0      0
sctp_session              0      0   1600     5    2 : tunables   60   30    0 : slabdata      0      0      0
tcp_session               3      5   1500     5    2 : tunables   60   30    0 : slabdata      1      1      0
ip_session                1      3   1200     3    1 : tunables   60   30    0 : slabdata      1      1      0
...
```

Which statement is true?

A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.
B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.
C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Answer: D

NEW QUESTION 51
During which phase of IKEv2 does the Diffie-Helman key exchange take place?

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

Answer: D

NEW QUESTION 55
Refer to the exhibit.

Debug output

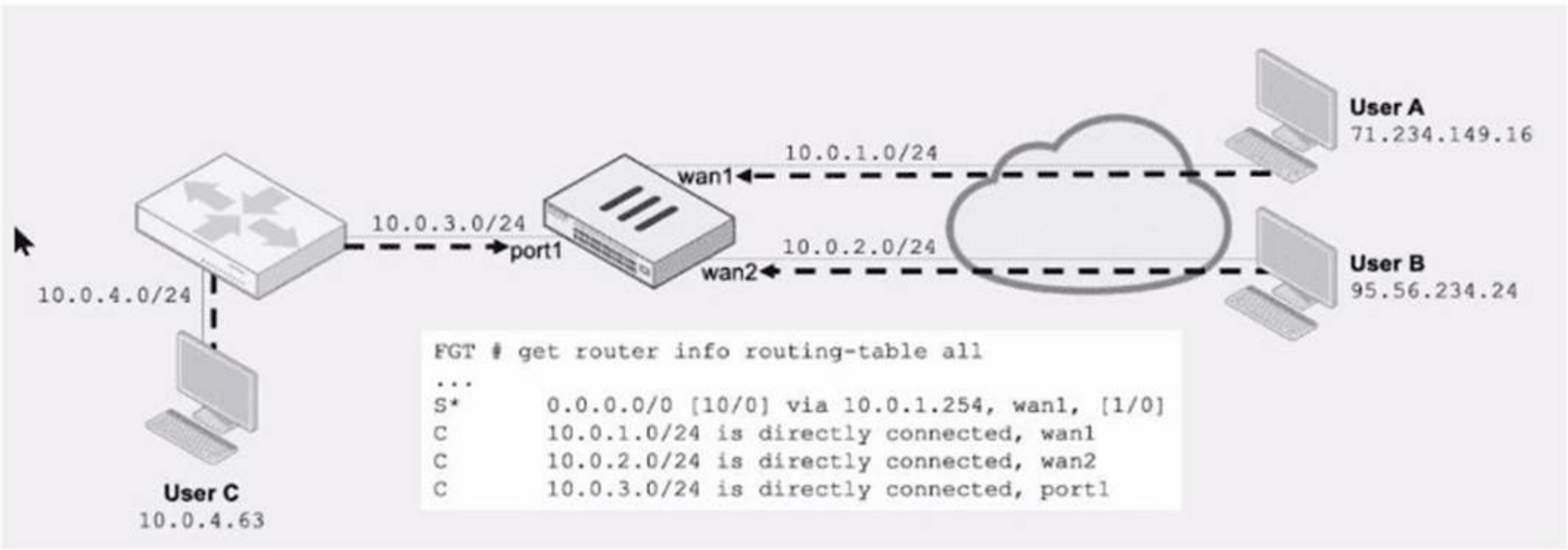
```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B708100050019E253B8B0000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF68F6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D890A367DBDDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:b1dd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E38196550C41FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBDC0000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84E6A79622FC1D44BC7F964986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA990000000 2C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A833800000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43118695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

An IPsec VPN tunnel is dropping, as shown by the debug output. Analyzing the debug output, what could be causing the tunnel to go down?

A. Phase 2 drops but Phase 1 is up.
B. Dead Peer Detection is not receiving its acknowledge packet.
C. The tunnel drops during rekey negotiation.
D. The tunnel drops after the timer expires.

Answer: B

NEW QUESTION 60
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 65
In the SAML negotiation process, which section does the Identity Provider (IdP) provide the SAML attributes utilized in the authentication process to the Service Provider (SP)?

A. SP Login dump
B. Authentication Response
C. Authentication Request
D. Assertion dump

Answer: D

NEW QUESTION 66
What are two functions of automation stitches? (Choose two.)

A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Answer: BD

NEW QUESTION 70
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 71
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 _ENCnone
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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
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 75

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

FCSS_NST_SE-7.6 Practice Exam Features:

* FCSS_NST_SE-7.6 Questions and Answers Updated Frequently

* FCSS_NST_SE-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_NST_SE-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_NST_SE-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year