Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
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 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
```

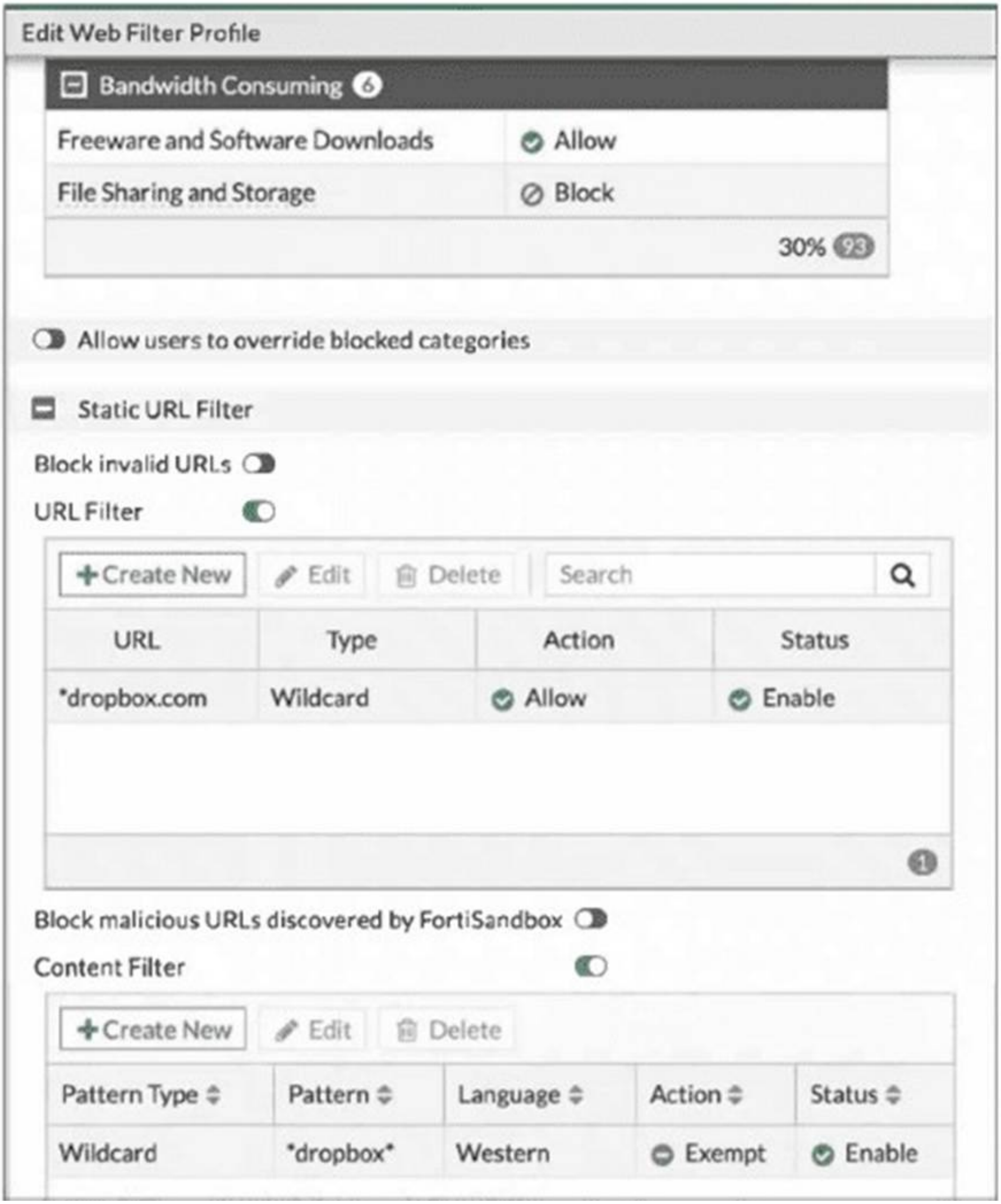
If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

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
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 4
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 5
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 6
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 7
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 8
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 8GP 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.

A.

Answer: D

Explanation:
The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show 'Idle,' 'Active,' or 'Connect,' but instead shows 'Established,' 'Up,' or related counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.
The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

NEW QUESTION 9
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 10
Refer to the exhibit.

**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><sa
ml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL3OW5sAZtBwhhEEtQF0AdfTN0u0GRr22%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.
Based on this output, what can you conclude?
A. Active Directory is used for authentication.
B. The authentication request is for an SSL VPN connection.
C. The IdP IP address is 10.1.10.254.
D. The IdP IP address is 10.1.10.2.

A.

Answer: D

NEW QUESTION 10
Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:          trans_id = KEY_IKE.
ike 0:624000:98:          encapsulation = IKE/none
ike 0:624000:98:                type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:                type OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:                type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:          trans_id = KEY_IKE.
ike 0:624000:98:          encapsulation = IKE/none
ike 0:624000:98:                type OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:                type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:                type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id - ISAKMP:
ike 0:624000:98:          trans_id = KEY_IKE.
ike 0:624000:98:          encapsulation = IKE/none
ike 0:620000:98:                type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:                type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:                type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:          trans_id = KEY_IKE.
ike 0:624000:98:          encapsulation = IKE/none
ike 0:624000:98:                type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:                type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:                type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.
Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.
B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
C. In the phase 1 network configuration, set the IKE version to 2.
D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Answer: A

NEW QUESTION 15
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 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

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349
From the snippet we can see that FortiGate (via the fssod daemon) is directly detecting the user logon rather than relying on a separate ??collector?? or ??DC agent.?? This indicates agentless polling—FortiGate polls the DC??s event logs over TCP 445 to discover logons. So: - FSSO is using agentless polling mode to detect logon events - In agentless mode, FortiGate will periodically poll the same IP (the DC) on port 445 to see if the user is still logged on

NEW QUESTION 17
Refer to the exhibit, which shows the partial output of command diagnose debug rating.

```
-=- Server List (Mon May  6 03:47:52 2024) -=-
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  6 03:47:43 2024
64.26.151.35                             10     46          -5                329072         0       6806 Mon May  6 03:47:43 2024
66.117.56.37                             10     75          -5                 71638         0        275 Mon May  6 03:47:43 2024
65.210.95.240                            20     71          -8                 36875         0         92 Mon May  6 03:47:43 2024
209.22.147.36                            20    103 DI       -8                 34784         0       1070 Mon May  6 03:47:43 2024
208.91.112.194                           20    107 D        -8                 35170         0       1533 Mon May  6 03:47:43 2024
96.45.33.65                              60    144           0                 33720         0        120 Mon May  6 03:47:43 2024
80.85.69.41                              71    226           1                 33797         0        192 Mon May  6 03:47:43 2024
62.209.40.74                            150     97           9                 33754         0        145 Mon May  6 03:47:43 2024
121.111.236.179                          45     44  F        -5                 26410     26226      26227 Mon May  6 03:47:43 2024
```

A. 66.117.56.37
B. 208.91.112.194
C. 209.22.147.36
D. 64.26.151.37

Answer: D

NEW QUESTION 19
Which statement about IKEv2 is true?

A. Both IKEv1 and IKEv2 share the feature of asymmetric authentication.
B. IKEv1 and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1 and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1 and IKEv2 share the concept of phase1 and phase2.

Answer: B

NEW QUESTION 24
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 28
Exhibit.

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
   <2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
    FGVM010000077649(updated 4 seconds ago): in-sync
    FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649(updated 4 seconds ago):
        sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
    FGVM010000077650(updated 1 seconds ago):
        sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
    FGVM010000077649(updated 4 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
    FGVM010000077650(updated 1 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary     : NGFW-1          , FGVM010000077649, HA cluster index = 1
Secondary   : NGFW-2          , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

Refer to the exhibit, which shows the output of get system ha status. NGFW-1 and NGFW-2 have been up for a week.
Which two statements about the output are true? (Choose two.)

A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.
B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.
C. If FGVM...649 is reboote
D. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
E. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Answer: BC

NEW QUESTION 31
Refer to the exhibit, which shows the output o! the BGP database.

```
router info bgp network
0 BGP table version is 3, local router ID is 1.1.1.1
tus codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           S Stale
gin codes: i - IGP, e - EGP, ? - incomplete


Network          Next Hop            Metric     LocPrf Weight RouteTag Path
.0.0.0/0         100.64.2.254    0               100      0         0 ? <-/->
                 100.64.2.1                           32768         0 ? <-/1>
.2.2.1/32        100.64.2.1                           32768         0 ? <-/1>
.8.8.8/32        100.64.2.254    0                100      0         0 ? <-/1>
10.20.30.0/24    172.16.54.115   0                100      0         0 i <-/1>


l number of prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0'24 was configured using the network command.
B. The first four prefixes are being advertised using a legacy route advertisement.
C. The advertised prefix of 10.20.30.0'24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: AD

NEW QUESTION 34
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 qwy=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 36
Refer to the exhibit, which shows a partial 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_FCDN-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 user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.
B. FortiOS performs a bind to the LDAP server using the user's credentials.
C. FortiOS collects the user group information.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: AD

NEW QUESTION 39
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 44
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 46

.....

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