Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1

View the exhibit, which contains the output of get sys ha status, and then answer the question below.

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
  <2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
  <2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649(updated 1 seconds ago): in-sync
  FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
  FGVM010000077649(updated 1 seconds ago):
    sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
  FGVM010000077650(updated 0 seconds ago):
    sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
  FGVM010000077649(updated 1 seconds ago):
    port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
  FGVM010000077650(updated 0 seconds ago):
    port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW      , FGVM010000077649
Slave : NGFW-2    , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM0100000077649
Slave :1 FGVM0100000077650
```

Which statements are correct regarding the output? (Choose two.)

A. The slave configuration is not synchronized with the master.
B. The HA management IP is 169.254.0.2.
C. Master is selected because it is the only device in the cluster.
D. port 7 is used the HA heartbeat on all devices in the cluster.

Answer: AD

NEW QUESTION 2

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
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
```

Which one of the following statements is true regarding FortiGate's inspection of this session?

A. FortiGate applied proxy-based inspection.
B. FortiGate forwarded this session without any inspection.
C. FortiGate applied flow-based inspection.
D. FortiGate applied explicit proxy-based inspection.

Answer: A

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 3

Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
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 tup
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.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
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
```

A. It is an ICMP session from 10.1.10.10 to 10.200.5. 1.
B. It is a TCP session in close_wait state, from 10.
C. 10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

Answer: A

NEW QUESTION 4
When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

A. FortiGate uses the requested URL from the user's web browser.
B. FortiGate uses the CN information from the Subject field in the server certificate.
C. FortiGate blocks the request without any further inspection.
D. FortiGate switches to the full SSL inspection method to decrypt the data.

Answer: B

NEW QUESTION 5
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, 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 inervals 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 send 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 local FortiGate OSPF router ID is 0.0.0.4.
B. Port4 is connected to the OSPF backbone area.
C. In the network connected to port4, two OSPF routers are down.
D. The local FortiGate is the backup designated router.

Answer: AB

Explanation:
Area 0.0.0.0 is the backbone area.

NEW QUESTION 6
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: ….: 75: responder: aggressive mode get 1ˢᵗ message…

…

ike 0: ….:76: incoming proposal:
ike 0: ….:76: proposal id = 0:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:     trans_id = KEY_IKE.
ike 0: ….:76:     encapsulation = IKE/none
ike 0: ….:76:        type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: my proposal, gw Remote:
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:     trans_id= KEY_IKE.
ike 0: ….:76:     encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val= PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val =MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:     trans_id= KEY_IKE.
ike 0: ….:76:     encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP1536.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: ….:76: no SA proposal chosen
```

Why didn't the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.
B. The remote gateway's Phase-2 configuration does not match the local gateway's phase-2 configuration.
C. The remote gateway's Phase-1 configuration does not match the local gateway's phase-1 configuration.
D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Answer: C

NEW QUESTION 7
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:9268ab9dea63aa3/0000000000000000:591: responder: main mode get 1st message...

ike 0:9268ab9dea63aa3/0000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/0000000000000000:591:       protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:          trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:          encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id=0:
ike 0:9268ab9dea63aa3/0000000000000000:591:       protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:          trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:          encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:             type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISA KMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: my proposal, gw VPN:
ike 0:9268ab9dea63aa3/0000000000000000:591:       proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:          protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:             trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:             encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:          protocol_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:             trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:             encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:          protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:             trans_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:             encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:                type= OAKLEY_ENCRYPT_ALG, val =AES-CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:                type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
```

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

A. Change phase 1 encryption to 3DES and authentication to SHA128.
B. Change phase 1 encryption to AES128 and authentication to SHA512.
C. Change phase 1 encryption to AESCBC and authentication to SHA2.
D. Change phase 1 encryption to AES256 and authentication to SHA256.

Answer: D

NEW QUESTION 8
Refer to the exhibit, which contains the output of get system ha status. Which two statements about the output are true? (Choose two.)

```
NGFW-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 2
Debug: 0
Cluster Uptime: 0 days 4:23:19
Cluster state change time: 2019-01-25 10:19:46
Master selected using:
    <2019/01/25 10:19:46> FGVM010000077649 is selected as the master because it has the largest value
of override priority.
    <2019/01/25 10:19:40> FGVM010000077649 is selected as the master because it's the only member in
the cluster.
ses_pickup: disable
override: enable
Configuration Status:
    FGVM010000077649 (updated 1 seconds ago): in-sync
    FGVM010000077650 (updated 0 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649 (updated 1 seconds ago):
        sessions=27, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=56%
    FGVM010000077650 (updated 0 seconds ago):
        sessions=2, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=57%
HBDEV stats:
    FGVM010000077649 (updated 1 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=63817615/202024/0/0, tx=
71110281/121109/0/0
    FGVM010000077650 (updated 0 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=79469596/122024/0/0, tx=
30877890/107878/0/0
Master: NGFW-1      , FGVM010000077649, cluster index = 1
Slave : NGFW-2      , FGVM010000077650, cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master: FGVM010000077649, operating cluster index = 0
Slave : FGVM010000077650, operating cluster index = 1
```

A. The slave configuration is synchronized with the master.
B. port7 is used as the HA heartbeat on all devices in the cluster.
C. Primary is selected based on the priority configured under config system ha.
D. The HA management IP is 169.254.0.2.

Answer: BC

NEW QUESTION 9
What does the dirty flag mean in a FortiGate session?

A. Traffic has been blocked by the antivirus inspection.
B. The next packet must be re-evaluated against the firewall policies.
C. The session must be removed from the former primary unit after an HA failover.
D. Traffic has been identified as from an application that is not allowed.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1

NEW QUESTION 10
View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.

```
NGFW-1 # diagnose sys session stat
misc info:     session_count=591  setup_rate=0  exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush-0, dev_down=0/0
TCP sessions:
        166 in NONE state
        1 in ESTABLISHED state
        3 in SYN_SENT state
        2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

Which statements are correct regarding the output shown? (Choose two.)

A. There are 0 ephemeral sessions.
B. All the sessions in the session table are TCP sessions.
C. No sessions have been deleted because of memory pages exhaustion.
D. There are 166 TCP sessions waiting to complete the three-way handshake.

Answer: AC

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578

NEW QUESTION 10
How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

A. FortiManager can download and maintain local copies of FortiGuard databases.
B. FortiManager supports only FortiGuard push to managed devices.
C. FortiManager will respond to update requests only if they originate from a managed device.
D. FortiManager does not support rating requests.

Answer: A

NEW QUESTION 13
An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any 'udp port 500'
B. diagnose sniffer packet any 'udp port 4500'
C. diagnose sniffer packet any 'esp'
D. diagnose sniffer packet any 'udp port 500 or udp port 4500'

Answer: C

Explanation:
Capture IKE Traffic without NAT:diagnose sniffer packet 'host and udp port 500'
——-Capture ESP
Traffic without NAT:diagnose sniffer packet any 'host and esp'
——-Capture IKE
and ESP with NAT-T:diagnose sniffer packet any 'host and (udp port 500 or udp port 4500)'

NEW QUESTION 18
Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; than answer the question below.

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag= 00000000 sockport=0 av_idx=0 use=3¶
origin-shaper=¶
reply-shaper=¶
per-ip_shaper=¶
ha_id=0 policy_dir=1 tunnel=/¶
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)¶
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial1=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd type=0 dd_mode=0¶
```

Which statement is true regarding the session in the exhibit?

A. It was created by the FortiGate kernel to allow push updates from FotiGuard.
B. It is for management traffic terminating at the FortiGate.
C. It is for traffic originated from the FortiGate.
D. It was created by a session helper or ALG.

Answer: D

NEW QUESTION 20
Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

A. Primary unit stops sending HA heartbeat keepalives.
B. The FortiGuard license for the primary unit is updated.
C. One of the monitored interfaces in the primary unit is disconnected.
D. A secondary unit is removed from the HA cluster.

Answer: AC

NEW QUESTION 24
An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.

```
#    debug application fnbamd -1
#    diagnose debug enable
#    diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

A. User student is not found in the LDAP server.
B. User student is using a wrong password.
C. The FortiGate has been configured with the wrong password for the LDAP administrator.
D. The FortiGate has been configured with the wrong authentication schema.

Answer: A

NEW QUESTION 28
Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Installing configuration changes to managed devices
B. Importing interface mappings from managed devices
C. Adding devices to FortiManager
D. Previewing pending configuration changes for managed devices

Answer: AD

NEW QUESTION 31

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

A. Group ID.
B. Group name.
C. Session pickup.
D. Gratuitous ARPs.

Answer: A

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

NEW QUESTION 34

Examine the IPsec configuration shown in the exhibit; then answer the question below.

Name	Remote
Comments	Comments

Network
IP Version   ● IPv4   ○ IPv6
Remote Gateway   Static IP Address ☑
IP Address   10.0.10.1
Interface   port1 ☑
Mode Config   ☐
NAT Traversal   ☑
Keepalive Frequency   10
Dead Peer Detection   ☑

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: diagnose vpn ike log-filter src-addr4 10.0.10.1 diagnose debug application ike -1 diagnose debug enable
The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

A. The IKE real time shows the phases 1 and 2 negotiations onl
B. It does not show any more output once the tunnel is up.
C. The log-filter setting is set incorrectl
D. The VPN's traffic does not match this filter.
E. The IKE real time debug shows the phase 1 negotiation onl
F. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
G. The IKE real time debug shows error messages onl
H. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: B

NEW QUESTION 36

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

```
#  diagnose ip router bgp all enable
#  diagnose ip router bgp level info
#  diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byt
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP peers have successfully interchanged Open and Keepalive messages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer is OpenConfirm.
D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 41
View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
# diagnose debug rating
Locale        : english
License       : Contract
Expiration    : Thu Sep 28 17:00:00 20xx
-=- Server List (Thu Apr 19 10:41:32 20xx) -=-
IP               Weight  RTT  Flags  TZ  Packets  Curr Lost  Total Lost
64.26.151.37     10      45          -5  262432   0          846
64.26.151.35     10      46          -5  329072   0          6806
66.117.56.37     10      75          -5  71638    0          275
65.210.95.240    20      71          -8  36875    0          92
209.222.147.36   20      103  DI     -8  34784    0          1070
208.91.112.194   20      107  D      -8  35170    0          1533
96.45.33.65      60      144         0   33728    0          120
80.85.69.41      71      226         1   33797    0          192
62.209.40.74     150     97          9   33754    0          145
121.111.236.179  45      44   F      -5  26410    26226      26227
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
B. Servers with the D flag are considered to be down.
C. Servers with a negative TZ value are experiencing a service outage.
D. FortiGate used 209.222.147.3 as the initial server to validate its contract.

Answer: AD

Explanation:
A – because flag is Failed so fortigate will check if server is available every 15 minD-state is I , contact to validate contract info

NEW QUESTION 44
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

A. FortiGate uses CN information from the Subject field in the server's certificate.
B. FortiGate switches to the full SSL inspection method to decrypt the data.
C. FortiGate blocks the request without any further inspection.
D. FortiGate uses the requested URL from the user's web browser.

Answer: A

NEW QUESTION 49
Refer to the exhibit, which contains the debug output of diagnose dvm device list.

```
FMG-VM64# diagnose dvm device list
There are currently 1 devices/vdoms managed:
TYPE    OID   SN       HA    IP            NAME           ADOM       IPS FIRMWARE
fmg/    217   FGVM01…  -     10.200.1.1    Local-FortiGate  My_ADOM 15.0.0831 6.0 MR4 (1579)
faz enabled                                                          (regular)
        |- STATUS: db: modified; conf: in sync; cond: pending; dm: retrieved;  conn: up

        |- vdom: [3] root flags:0 adom:My_ADOM pkg: [imported] Local-FortiGate_root
```

Which two statements about the output shown in the exhibit are correct? (Choose two.)

A. ADOMs are disabled on the FortiManager
B. The FortiGate configuration is in sync with latest running revision history.
C. There are pending device-level changes yet to be installed on Local-FortiGate.
D. The policy package has been modified for Local-FortiGate.

Answer: BC

NEW QUESTION 54
A FortiGate device has the following LDAP configuration:

```
config user ldap
    edit "WindowsLDAP"
        set server "10.0.1.10"
        set cnid "cn"
        set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
        set type regular
        set username "dc=trainingAD, dc=training, dc=lab"
        set password xxxxxxx
    next
end
```

The administrator executed the 'dsquery' command in the Windows LDAp server 10.0.1.10, and got the following output:
>dsquery user –samid administrator
"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.
B. username.
C. password.
D. dn.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

NEW QUESTION 55
Examine the output of the 'get router info ospf neighbor' command shown in the exhibit; then answer the question below.

```
# get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State        Dead Time    Address         Interface
0.0.0.69          1   Full/DR      00:00:32     10.126.0.69     wan1
0.0.0.117         1   Full/DROther 00:00:34     10.126.0.117    wan1
0.0.0.2           1   Full/ -      00:00:36     172.16.1.2      ToRemote
```

Which statements are true regarding the output in the exhibit? (Choose two.) Refer to the exhibit, which shows the output of a debug command.
Which statement about the output is true?

A. TheOSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wa
B. l network.
C. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
D. The local FortiGate is the designated router for the wan1 network.
E. The interface ToRemote is a point-to-point OSPF network.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

NEW QUESTION 58
What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

A. av-failopen
B. mem-failopen
C. utm-failopen
D. ips-failopen

Answer: A

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideratio

NEW QUESTION 62
Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concervemode: 0
shm last entered: n/a
system last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912

SHM FS alloc: 7110656
```

Which of the following statements are true regarding the above outputs? (Choose two.)

A. The unit is running a 32-bit FortiOS
B. The unit is in kernel conserve mode
C. The Cached value is always the Active value plus the Inactive value
D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: AC

NEW QUESTION 64
View the IPS exit log, and then answer the question below.
# diagnose test application ipsmonitor 3 ipsengine exit log"
pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual
What is the status of IPS on this FortiGate?

A. IPS engine memory consumption has exceeded the model-specific predefined value.
B. IPS daemon experienced a crash.
C. There are communication problems between the IPS engine and the management database.
D. All IPS-related features have been disabled in FortiGate's configuration.

Answer: D

Explanation:
The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes.Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated:Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-releated features have been disabled)

NEW QUESTION 66
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

Which statement are true regarding the output in the exhibit? (Choose two.)

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
C. FortiGate will send the FortiGuard queries to the server with highest weight.
D. A server's round trip delay (RTT) is not used to calculate its weight.

Answer: BC

NEW QUESTION 67
Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
B. SIP ALG supports SIP HA failover; SIP helper does not.
C. SIP ALG supports SIP over IPv6; SIP helper does not.
D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer: BCD

NEW QUESTION 72
When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.
B. The server requires more information from the user, such as the token code for two-factor authentication.
C. The user credentials are wrong.
D. The user account is not found in the server.

Answer: B

NEW QUESTION 75
Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

A. The link health monitor (if configured) is up.
B. There is no other route, to the same destination, with a higher distance.
C. The outgoing interface is up.
D. The next-hop IP address is up.

Answer: AC

NEW QUESTION 78
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. Neighbor range
B. Route reflector
C. Next-hop-self
D. Neighbor group

Answer: B

Explanation:
Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routers learned from one peer to the other peers. If you configure route reflectors, you dont' need to create a full mesh IBGP network. All clients in a cluster only talck to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

NEW QUESTION 83
Refer to the exhibit, which shows a FortiGate configuration.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers 1
    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-mpercent 2
    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-ip6 ::
    set proxy-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username ''
    set ddns-server-ip 0.0.0.0
    set ddns-server-port 443
end
```

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 change to fix the issue?

A. The administrator must increase webfilter-timeout.
B. The administrator must disable webfilter-force-off.
C. The administrator must change protocol to TCP.
D. The administrator must enable fortiguard-anycast.

Answer: D

NEW QUESTION 85
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:H2S_0_1:1249: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_1:  recv shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 13 10.1.1.254->10.1.2.254 route lookup oif 13
ike 0:H2S_0_0: forward shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-ma
ike 0:H2S_0_0:1248: sent IKE msg (SHORTCUT-QUERY): 100.64.1.1:500->100.64.5.1:500, len=236,
id=e2beec89f13c7074/06a73dfb3a5d3b54:340a645c
ike 0: comes 100.64.5.1:500->100.64.1.1:500, ifindex=3. . .
ike 0: IKEv1 exchange=Informational id=e2beec89f13c7074/06a73dfb3a5d3b5d:26254ae9 len=236
ike 0:H2S_0_0:1248: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 13.10.1.2.254->10.1.1.254 route lookup
ike 0:H2S 0 1: forward shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.
```

Based on the debug output, which phase 1 setting is enabled in the configuration of this VPN?

A. auto-discovery-shortcut
B. auto-discovery-forwarder
C. auto-discovery-sender
D. auto-discovery-receiver

Answer: D

NEW QUESTION 87
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0: comes 10.0.0.2:500-> 10.0.0.1:500, ifindex-7..
ike 0: IKEV1 exchange-Aggressive id-baf47d0988e9237f/2f405ef3952f6fda len 430
ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA011004000000000000001AE0400003C0000000100000001000000300101000
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD AFCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:     protocol id = ISAKMP:
ike 0: RemoteSite:4:         trans_id = KEY_IKE.
ike 0: RemoteSite:4:         encapsulation = IKE/none
ike 0: RemoteSite:4:             type=OAKLEY_ENCRYPT_ALG,  val=AES_CBC, key-len=128
ike 0: RemoteSite:4:             type=OAKLEY_HASH_ALG, val=SHA
ike 0: RemoteSite:4:             type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:             type=OAKLEY_GROUP, val=MODP1024.
ike 0: RemoteSite:4: ISAKMP SA lifetime=86400
ike 0: RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key
16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0: RemoteSite:4: PSK authentication succeeded
ike 0: RemoteSite:4: authentication OK
ike 0: RemoteSite:4: add INITIAL-CONTACT
ike 0: RemoteSite:4: enc
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000080140000181F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_i2send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

Which statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.
B. It shows a phase 1 negotiation.
C. The negotiation is using AES128 encryption with CBC hash.
D. The initiator has provided remote as its IPsec peer ID.

Answer: BD

NEW QUESTION 89
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. FortiGate first checks the OSPF ID to elect a DR.
B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
C. BDR is responsible for forwarding link state information from one router to another.
D. Only the DR receives link state information from non-DR routers.

Answer: B

NEW QUESTION 90
In which two states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.
B. A TCP session waiting for FIN ACK.
C. A UDP session with packets sent and received.
D. A UDP session with only one packet received.

Answer: AD

NEW QUESTION 95
Which two statements about OCVPN are true? (Choose two.)

A. Only root vdom supports OCVPN.
B. OCVPN supports static and dynamic IPs in WAN interface.
C. OCVPN offers only Hub-Spoke VPNs.
D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: AB

NEW QUESTION 98
An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
C. Sends a link failed signal to all connected devices.
D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Answer: A

NEW QUESTION 103
View these partial outputs from two routing debug commands:

```
# 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=10.200.1.254
dev=2(port1)
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=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```
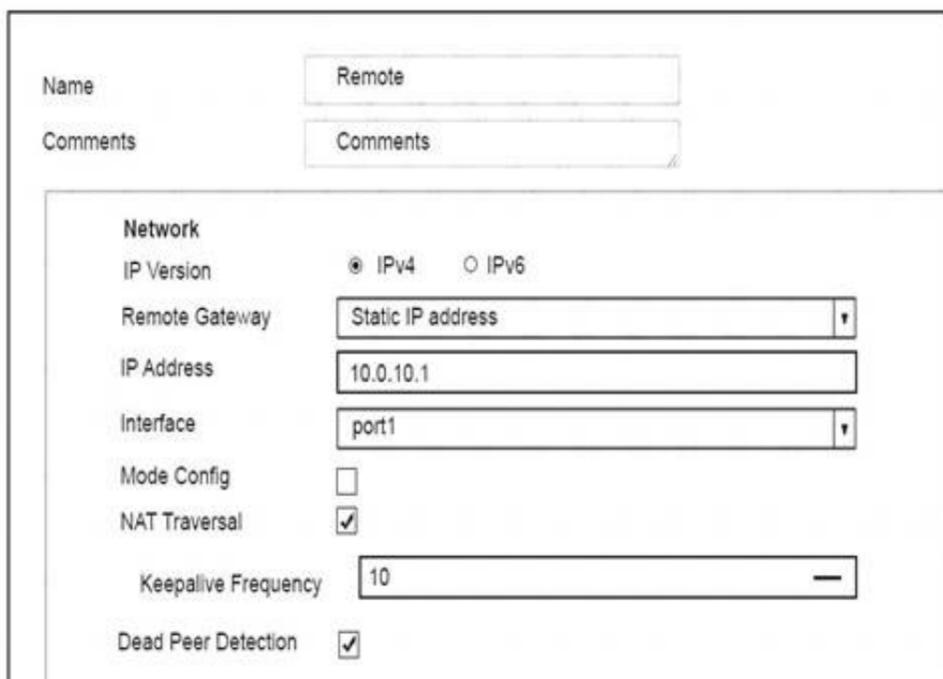
Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. Both port1 and port2
B. port3
C. port1
D. port2

Answer: C

NEW QUESTION 106
View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

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

A. The debug output shows phases 1 and 2 negotiations onl
B. Once the tunnel is up, it does not show any more output.
C. The log-filter setting was set incorrectl
D. The VPN's traffic does not match this filter.
E. The debug shows only error message
F. If there is no output, then the tunnel is operating normally.
G. The debug output shows phase 1 negotiation onl
H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 107
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
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
10.200.3.1    4  65501    101       115       0    0    0   never         Active

Total number of neighbors 3
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.
B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixes.

Answer: AC

NEW QUESTION 109
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0 -> 10.200.4.1:0
bound_if=3 lgwy-statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast-10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle-20000ms retry-3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
    src: 0:10.1.2.0/255.255.255.0:0
    dat: 0:10.1.1.0/255.255.255.0:0
    SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/OB replaywin=204B seqno=1
esn-replaywin_lastseq-00000000
    life: type=01 bytes=0/0 timeout=43177/43200
    dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
         ah-sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

Based on the output, which two statements are correct? (Choose two.)

A. Anti-replay is enabled.
B. DPD is disabled.
C. Remote gateway IP is 10.200.4.1.
D. Quick mode selectors are disabled.

Answer: AC

NEW QUESTION 112
View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which of the following statements is true regarding this output?

A. The requested URL belongs to category ID 255.
B. The server hostname Is training, fortinet.com.
C. FortiGate found the requested URL in its local cache.
D. This web request was inspected using the ftgd-allow web filter profile.

Answer: C

NEW QUESTION 115
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V    AS    MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.200.3.1  4  65501       92      112       0    0     0    never   Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
B. The TCP session for the BGP connection to 10.200.3.1 is down.
C. The local peer has received the BGP prefixed from the remote peer.
D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

Explanation:
http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4

NEW QUESTION 120
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 124
Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen
B. mem failopen
C. AV failopen
D. UTM failopen

Answer: AC

NEW QUESTION 128
......

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

NSE7_EFW-7.0 Practice Exam Features:

* NSE7_EFW-7.0 Questions and Answers Updated Frequently

* NSE7_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-7.0 Practice Test Here](https://www.surepassexam.com/NSE7_EFW-7.0-exam-dumps.html)