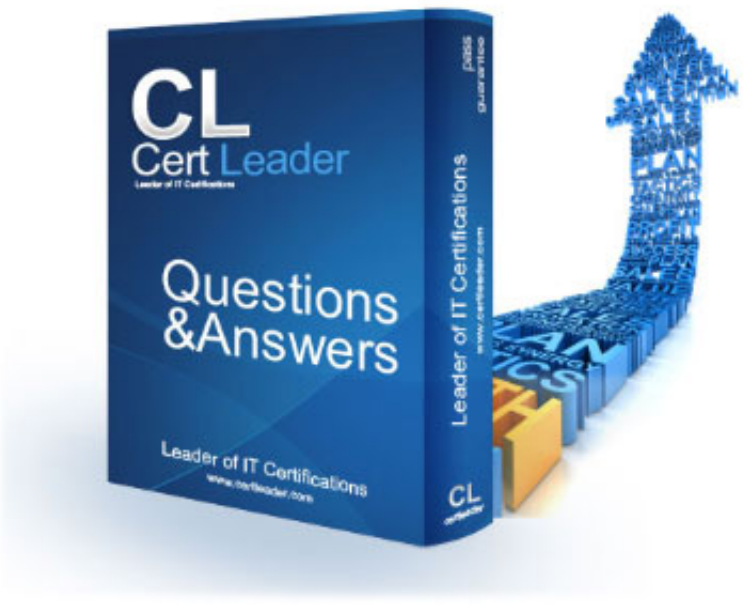
NSE7_EFW-7.0 Dumps

Fortinet NSE 7 - Enterprise Firewall 7.0

https://www.certleader.com/NSE7_EFW-7.0-dumps.html



NEW QUESTION 1
View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
FGT # 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
100.64.3.1    4 65501   101      115       0        0     0      never            Active

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

A. The local router's BGP state is Established with the 10.125.0.60 peer.
B. Since the counters were last reset; the 10.200.3.1 peer has never been down.
C. The local router has received a total of three BGP prefixes from all peers.
D. The local router has not established a TCP session with 100.64.3.1.

Answer: AD

NEW QUESTION 2
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 3
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.

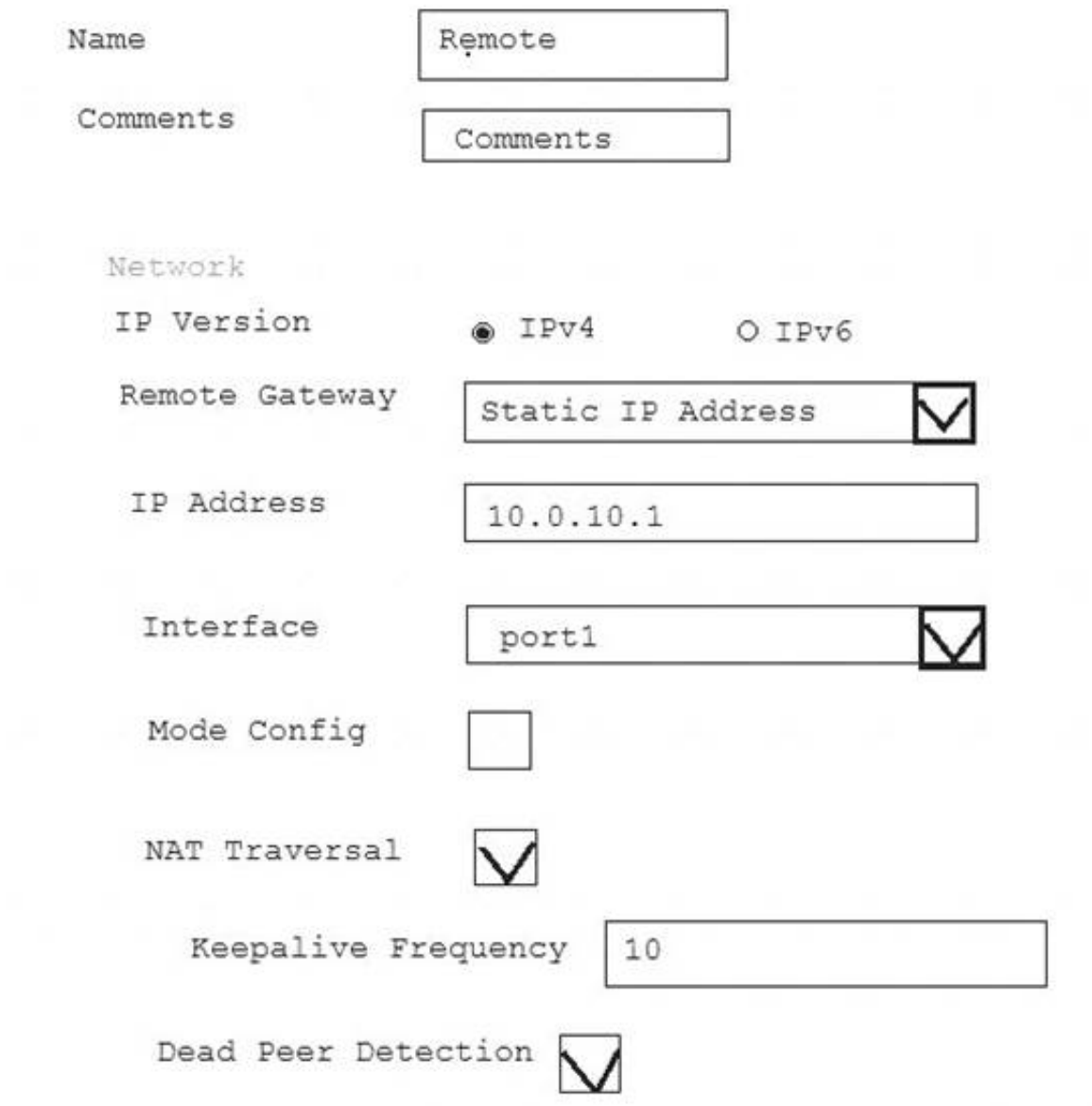
Answer: AC

NEW QUESTION 4
Which two statements about bulk configuration changes made using FortiManager CLI scripts are correct? (Choose two.)

A. When run on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate device.
B. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
C. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.
D. When run on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate device.

Answer: AB

NEW QUESTION 5
Examine the IPsec configuration shown in the exhibit; then answer the question below.



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 6
Refer to the exhibit, which shows a session table entry.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 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=redir local may_dirty none app_ntf
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=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)
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
rpdb_link_id = 00000000
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 statement about FortiGate behavior relating to this session is true?

A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
B. FortiGate forwarded this session without any inspection.
C. FortiGate is performing security profile inspection using the CP
D. FortiGate applied only IPS inspection to this session.

Answer: C

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 91, 92 First digit of "proto_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage

NEW QUESTION 7
Refer to the exhibit, which shows the output of diagnose sys session list.

```
# 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/ff 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 will happen if the primary fails and the secondary becomes the primary?

A. 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.
B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.
C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.
D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-see-if-a-session-is-synced-in-HA/ta-p/1941

NEW QUESTION 8
Refer to the exhibit, which contains the output of a BGP debug command.

```
FGT # 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
100.64.3.1      4 65501  101     115       0     0    0   never       Active

Total number of neighbors 3
```

Which statement about the exhibit is true?

A. The local router has received a total of three BGP prefixes from all peers.
B. The local router has not established a TCP session with 100.64.3.1.
C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

NEW QUESTION 9
A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.

B. Policy monitor.
C. Logs.
D. Crashlogs.

Answer: CD

NEW QUESTION 10
Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.1.254 dev=3(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9(port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
                  [10/0] via 100.64.2.254, port2, [10/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.10.0/24 [10/0] via 10.1.0.1, port3
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

A. Set the priority of the static default route using port1 to 10. Most Voted
B. Set the priority of the static default route using port2 to 1.
C. Set preserve-session-route to enable.
D. Set snat-route-change to enable.

Answer: A

Explanation:
ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.
https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/25967/equal-cost-multi-path

NEW QUESTION 10
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 11
An administrator wants to capture encrypted phase 2 traffic between two FortiGate 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 ‘ah’
B. diagnose sniffer packet any ‘ip proto 50’
C. diagnose sniffer packet any ‘udp port 4500’
D. diagnose sniffer packet any ‘udp port 500’

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p. 443 Phase 2 : ESP => IP protocol 50
This command will capture any packets that use the IP protocol number 50, which is ESP (Encapsulating Security Payload). ESP is used to encrypt and authenticate the phase 2 traffic between two FortiGate device1s.

NEW QUESTION 16
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 oif 13
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 18
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
     name: 'Hub2Spoke1'
     auto-negotiate: disable
     mode: tunnel
     src: 0:192.168.1.0/0.0.0.0:0
     dst: 0:10.10.20.0/0.0.0.0:0
     SA
       lifetime/rekey: 43200/32137
       mtu: 1438
       tx-esp-seq: 2ce
       replay: enabled
       inbound
         spi: 01e54b14
         enc:  aes-cb 914dc5d092667ed436ea7f6efb867976
         auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
       outbound
         spi: 3dd3545f
         enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
```

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

A. Phase 2 authentication is set to sha1 on both sides.
B. Anti-replay is disabled.
C. Hub2Spoke1 is a policy-based VPN.
D. Hub2Spoke1 is configured on interface wan2.

Answer: AD

NEW QUESTION 22
View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
    diagnose sys session list expectation

session info: proto=6 proto_state-00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-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
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

A. This is an expected session created by a session helper.
B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
D. This is an expected session created by an application control profile.

Answer: AC

NEW QUESTION 23
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 26
Examine the partial output from two web filter debug commands; then answer the question below:

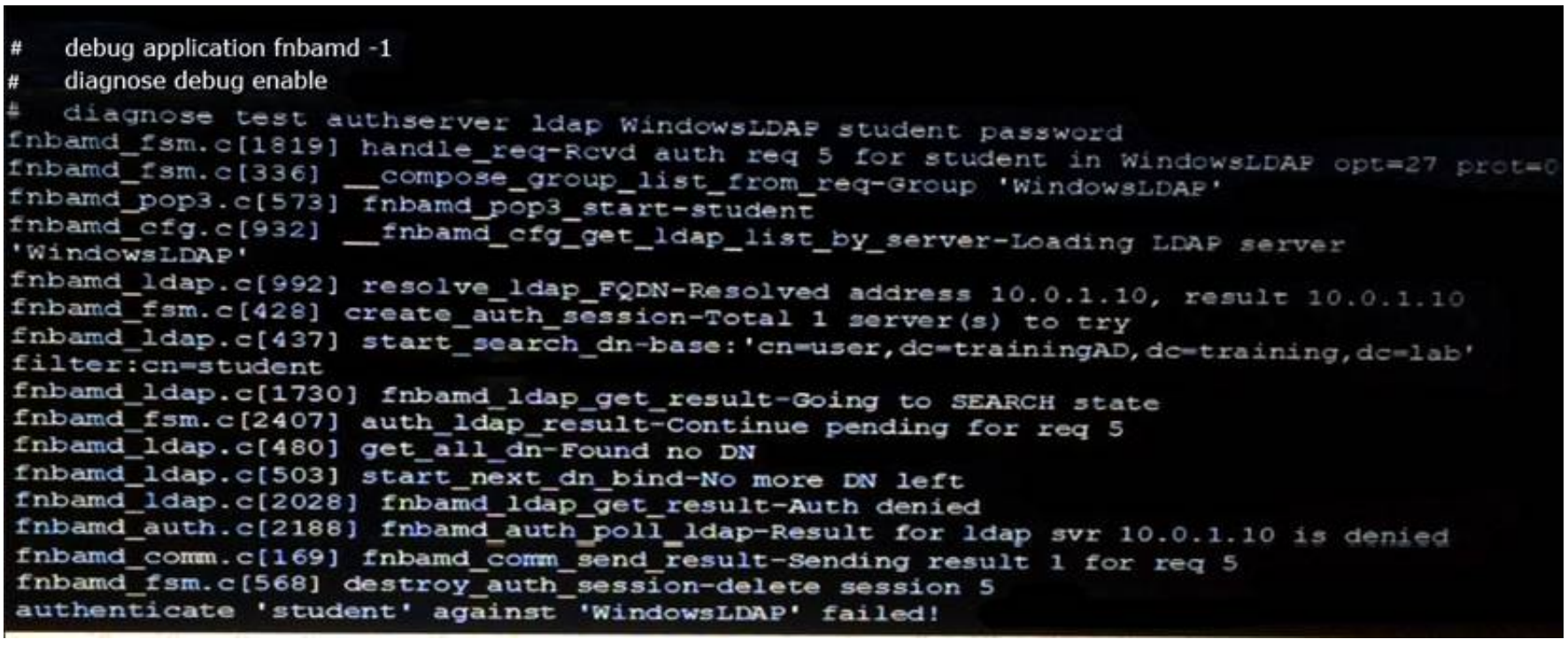
```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
  34 Finance and Banking
  37 Search Engines and Portals
  43 General Organizations
  49 Business
  50 Information and Computer Security
  51 Government and Legal Organizations
  52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking
B. General organization.
C. Business.
D. Information technology.

Answer: C

NEW QUESTION 31
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.



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 35
Which statement about protocol options is true?

A. Protocol options allows administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
B. Protocol options allows administrators the ability to configure the Any setting for all enabled protocols which provides the most efficient use of system resources.
C. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
D. Protocol options allows 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 36
What is the diagnose test application ipsmenitor 5 command used for?

A. To enable IPS bypass mode
B. To disable the IPS engine
C. To restart all IPS engines and monitors
D. To provide information regarding IPS sessions

Answer: A

Explanation:
diagnose test application ipsmonitor 5: Toggle bypass status
* 13: IPS session list
* 98: Stop all IPS engines
* 99: Restart all IPS engines and monitor

NEW QUESTION 37
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 42
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. route-reflector enable
B. route-reflector-server enable
C. route-reflector-client enable
D. route-reflector-peer enable

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/572620/config-router-bgp set route-reflector-client [enable|disable]

NEW QUESTION 44
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "portl"
set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=716
ike 0:xxx/xxx:16: responder: main mode get 1st message...
ike 0:xxx/xxx:16: VID RFC 3947 4A131C81070358455C5728F20E95452F
...
ike 0:xxx/xxx:16: negotiation result
ike 0:xxx/xxx:16: proposal id = 1:
ike 0:xxx/xxx:16:   protocol id = ISAKMP:
ike 0:xxx/xxx:16:     trans_id = KEY_IKE.
ike 0:xxx/xxx:16:     encapsulation = IKE/none
ike 0:xxx/xxx:16:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:xxx/xxx:16:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:xxx/xxx:16:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:xxx/xxx:16:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:xxx/xxx:16: ISAKMP SA lifetime=86400
ike 0:xxx/xxx:16: SA proposal chosen, matched gateway DialUpUsers
...
ike 0:DialUpUsers:16: sent IKE msg (ident_r1send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
```

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=380
ike 0:DialUpUsers:16: responder:main mode get 2nd message...
ike 0:DialUpUsers:16: NAT not detected
ike 0:DialUpUsers:16: sent IKE msg (ident_r2send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0:DialUpUsers:16: ISAKMP SA xxx/xxx key 16:3D33E2EF00BE927701B5C25B05A62415
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=108
ike 0:DialUpUsers:16: responder: main mode get 3rd message...
ike 0:DialUpUsers:16: probable pre-shared secret mismatch
ike 0:DialUpUsers:16: unable to parse msg
```

What is causing the IPsec problem in the phase 1 ?

A. The incoming IPsec connection is matching the wrong VPN configuration
B. The phrase-1 mode must be changed to aggressive
C. The pre-shared key is wrong
D. NAT-T settings do not match

Answer: C

NEW QUESTION 45
View the global IPS configuration, and then answer the question below.

```
config ips global
    set fail-open disable
    set intelligent-mode disable
    set engine-count 0
    set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.
B. FortiGate will spawn IPS engine instances based on the system load.
C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.
D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Answer: A

NEW QUESTION 46
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

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/1969

NEW QUESTION 47
An administrator has created a VPN community within VPN Manager on FortiManager. They also added gateways to the VPN community and are now trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces are not listed as available options.
What step must the administrator take to resolve this issue?

A. Install the VPN community and gateway configuration to the FortiGate devices, in order for the interfaces to be displayed within Policy & Objects on FortiManager
B. Set up all of the phase 1 settings in the VPN community that they neglected to set up initiall
C. The interfaces will be automatically generated after the administrator configures all of the required settings.
D. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.
E. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

Answer: A

Explanation:
* - Create a VPN Community 2- Install VPN Configuration 3- Add IPsec Firewall Policies 4- Install the Policies

NEW QUESTION 51
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 intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

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

A. In the network connected to port 4, two OSPF routers are down.
B. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.5.
C. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.6.
D. There are a total of 5 OSPF routers attached to the Port4 network segment.

Answer: BD

NEW QUESTION 53
What are two functions of automation stitches? (Choose two.)

A. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.

B. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.
C. Automation stitches can be created to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.
D. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

Answer: BC

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 23, 26

NEW QUESTION 54
Examine the following traffic log; then answer the question below.
date-20xx-02-01 time=19:52:01 devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted."
What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.
B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
C. FortiGate does not have any available NAT port for a new connection.
D. The limit for the maximum number of entries in the NAT port table has been reached.

Answer: B

NEW QUESTION 57
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. Increase webfilter-timeout.
B. Change protocol to TCP.
C. Enable fortiguard-anycast.
D. Disable webfilter-force-off.

Answer: D

NEW QUESTION 58
An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.
What can the administrator do to fix this problem?

A. Configure remote link monitoring to detect an issue in the forwarding path.
B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
D. Configure set link-failed-signal enable under config system ha on both cluster members.

Answer: D

Explanation:
Virtual MAC Address and Failover - The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port. - Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces): #Config system ha set link-failed-signal enable end - This simulates a link failure that clears the related entries from MAC table of the switches.

NEW QUESTION 62
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn't the tunnel come up?

A. The pre-shared keys do not match.
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. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Answer: C

NEW QUESTION 66
View the exhibit, which contains a partial routing table, and then answer the question below.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C       10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C       10.1.0.0/24 is directly connected, port3
S       10.10.4.0/24 [10/0] via 10.1.0.100, port3
C       10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S       10.1.0.0/24 [10/0] via 10.72.3.254, port4
C       10.72.3.0/24 is directly connected, port4
S       192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.

D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 71
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 75
Which statement about IKE and IKE NAT-T is true?

A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.
B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.
C. They both use UDP as their transport protocol and the port number is configurable.
D. They each use their own IP protocol number.

Answer: C

Explanation:
IKE without NAT-T runs over UDP port 500. IKE with NAT-T runs over UDP port 4500. It can be configurable - https://docs.fortinet.com/document/fortigate/7.0.0/new-features/33578/configurable-ike-port

NEW QUESTION 79
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 84
Which two statements about conserve mode are true? (Choose two.)

A. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
B. FortiGate starts dropping all new sessions when the system memory reaches the configured redthreshold.

C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
D. FortiGate exits conserve mode when the system memory goes below the configured green threshold.

Answer: AD

NEW QUESTION 86
Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

A. Diagnose debug application radius -1.
B. Diagnose debug application fnbamd -1.
C. Diagnose authd console –log enable.
D. Diagnose radius console –log enable.

Answer: B

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838

NEW QUESTION 89
Examine the output from the 'diagnose debug authd fsso list' command; then answer the question below.
diagnose debug authd fsso list —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is
NOT the one used by the workstation INTERNAL2. TRAINING. LAB.
What should the administrator check?

A. The IP address recorded in the logon event for the user STUDENT.
B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
C. LAB.
D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
E. LAB.
F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 91
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 94
Refer to the exhibit, which shows the output of a diagnose command

```
FGT # diagnose debug rating
Locale       : english
Service      : Web-filter
Status       : Enable
License      : Contract
Service      : Antispam
Status       : Disable
Service      : Virus Outbreak Prevention
Status       : Disable
 -=- Server List (Mon 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
```

What can you conclude from the RTT value?

A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.
B. Its value is incremented with each packet lost.
C. It determines which FortiGuard server is used for license validation.
D. Its initial value is statically set to 10.

Answer: A

NEW QUESTION 99
What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

A. Reduce the session time to live.
B. Increase the TCP session timers.
C. Increase the FortiGuard cache time to live.
D. Reduce the maximum file size to inspect.

Answer: AD

NEW QUESTION 104
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 106
The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

A. The CA cannot resolve the name of the workstation.
B. The FortiGate cannot resolve the name of the workstation.
C. The remote registry service is not running in the workstation 192.168.12.232.
D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548

NEW QUESTION 107
Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. set av-failopen off
B. set av-failopen pass
C. set fail-open enable
D. set ips fail-open disable

Answer: AC

Explanation:
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserve-mode

NEW QUESTION 109
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

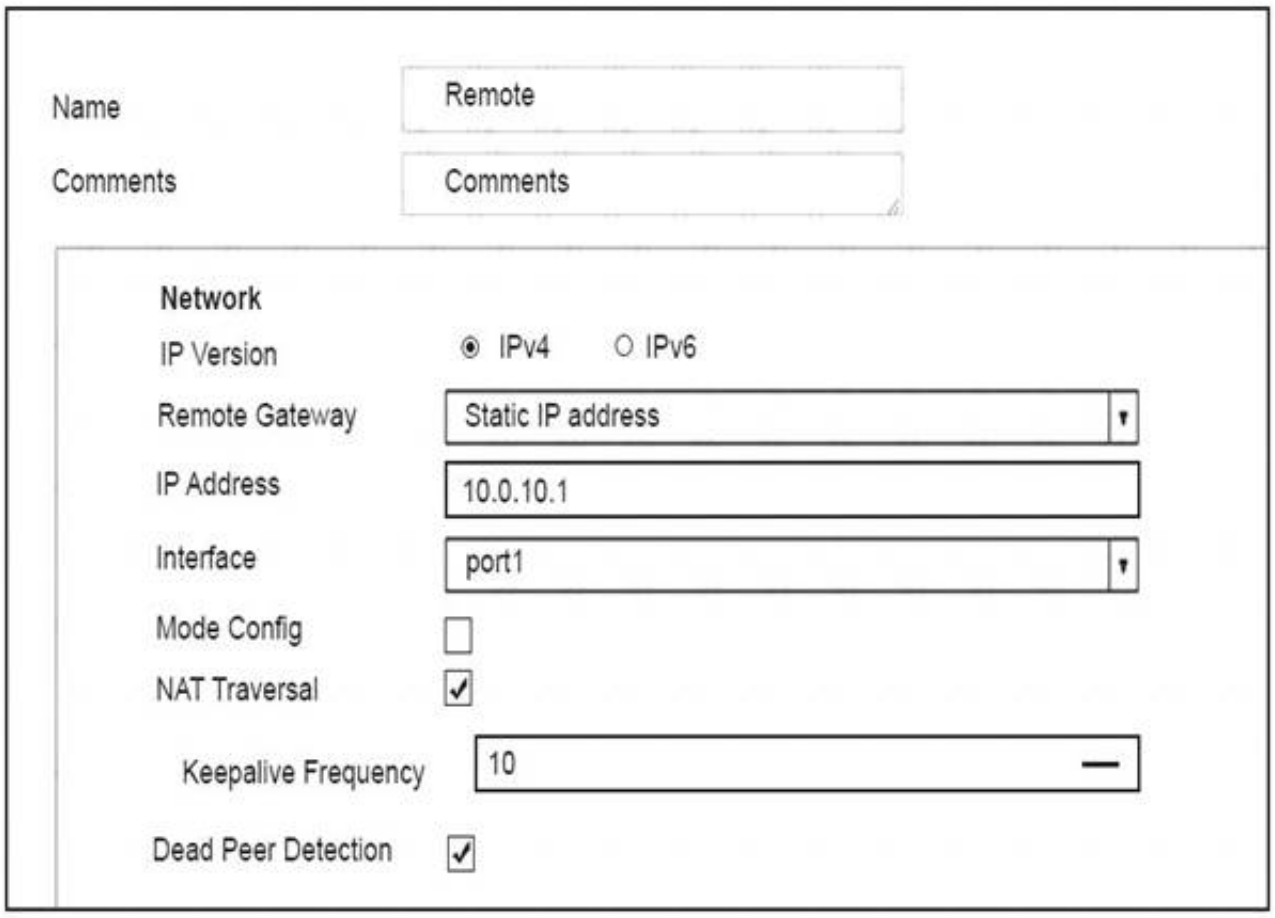
```
ike 0:9268ab9dea63aa3/0000000000000000:591: responder: main mode get 1st message…
…
ike 0:9268ab9dea63aa3/0000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:       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 111
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 115
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
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
iike 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
```

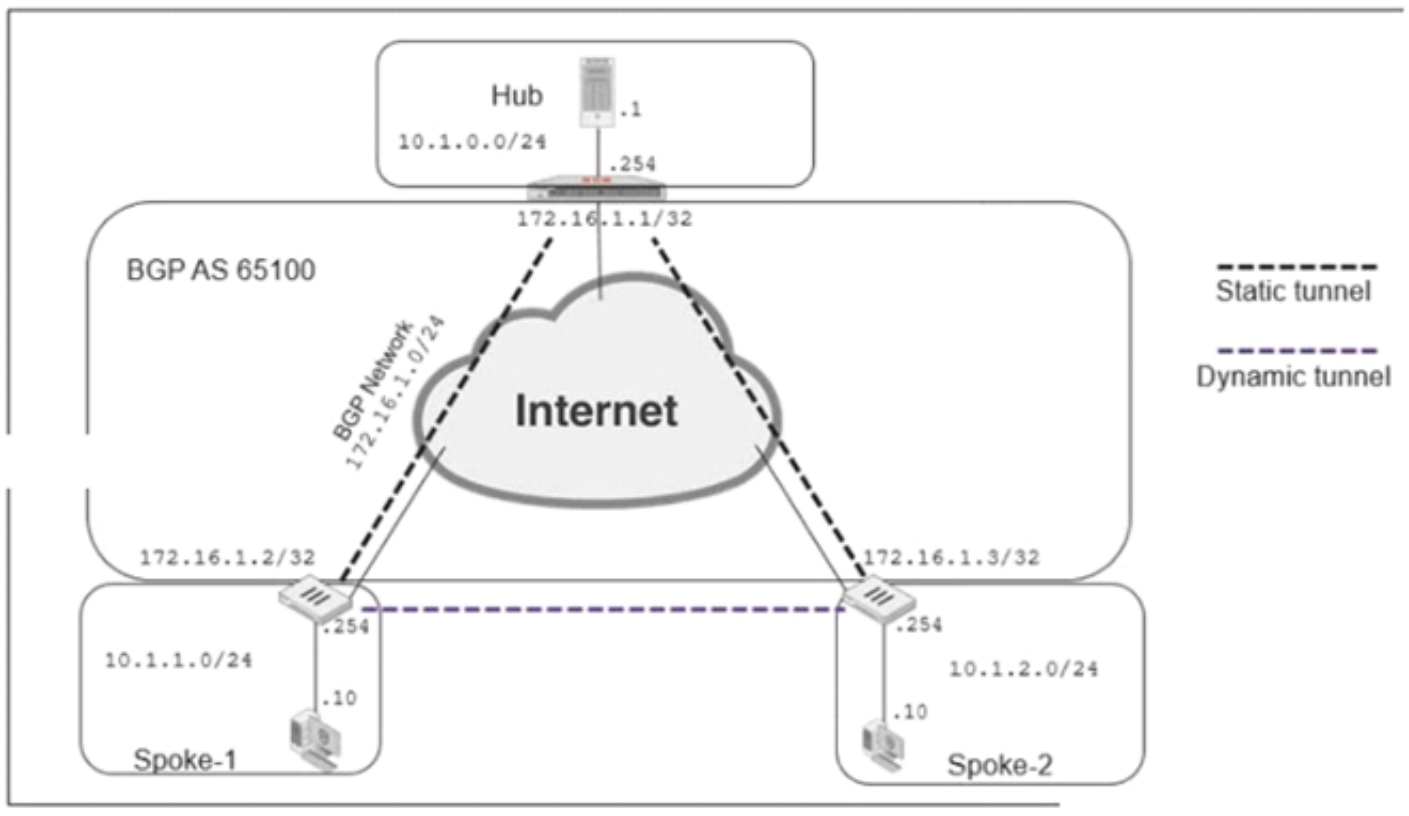
The administrator does not have access to the remote gateway.
Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

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

Answer: D

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852

NEW QUESTION 116
Exhibits:




```
how router bgp
router bgp
 as 65100
 router-id 172.16.1.1
fig neighbor-group
 edit "advpn"
     set remote-as 65100

     set route-reflector-client disable
 next

fig neighbor-range
 edit 1
     set prefix 172.16.1.0 255.255.255.0
     set neighbor-group "advpn"
 next
```

Refer to the exhibits, which contain the network topology and BGP configuration for a hub.
An administrator is trying to configure ADVPN with a hub-spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however, the spokes are not receiving route information from each other.
What change must the administrator make to the hub BGP configuration so that the routes learned by one
spoke are forwarded to the other spokes?

A. Configure an individual neighbor and remove neighbor-range configuration.
B. Configure the hub as a route reflector client.
C. Change the router id to 10.1.0.254.
D. Make the configuration of remote-as different from the configuration of local-as.

Answer: B

Explanation:
Source:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-BGP-route-reflector/ta-p/191503 Source 2: RFC 4456

NEW QUESTION 120
Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
……
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn't match the sniffer filter.
B. Number of total packets dropped by the FortiGate.
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.

D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=11655

NEW QUESTION 125
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
B. Only the root FortiGate sends logs to FortiAnalyzer.
C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

Answer: AC

Explanation:
FortiGate's to Root uses FortiTelemetry (TCP-8013) FortiTelemetry is also used for FortiClient communication Root Fortigate to FortiAnalyzer uses API (TCP-443)

NEW QUESTION 128
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 133
How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

A. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.
B. When run on the Device Database, changes are applied directly to the managed FortiGate device.
C. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device

Answer: CD

Explanation:
CLI scripts can be run in three different ways:Device Database: By default, a script is executed on the
device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.
Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.
Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don’t need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

NEW QUESTION 134
Refer to the exhibit, which shows the output of a debug command.

```
FGT # 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    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.
B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.
C. There are more than two OSPF routers on the wan2 network.
D. The interface ToRemote is a broadcast OSPF network.

Answer: C

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

NEW QUESTION 139
Refer to the exhibit, which contains the output of the diagnose vpn tunnel list. Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any 'esp and host 10.200.3.2'
B. diagnose sniffer packet any 'ip proto 50'
C. diagnose sniffer packet any 'host 10.0.10.10'
D. diagnose sniffer packet any 'port 4500'

Answer: D

NEW QUESTION 141
You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.
Which two settings need to be verified for these features to function? (Choose two.)

A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.
B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.
C. Service access needs to be enabled on FortiManager under System Settings > Network.
D. FortiGate needs to have include-default-servers disabled under config system central-management.

Answer: AC

Explanation:
NSE 7.0 Guide page 184-185

NEW QUESTION 146
Which two statements about application-layer test commands are true? (Choose two.)

A. Some of them display real-time application debugs.
B. Some of them can be used to restart an application.
C. Some of them display statistics and configuration information about a feature or process.
D. Some of them only display output, after you run the diagnose debug console enable command.

Answer: BC

NEW QUESTION 147
Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

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

Answer: CDE

Explanation:
A configured static route only goes to routing table from routing database when all the following are met :
- The outgoing interface is up
- There is no other matching route with a lower distance
- The link health monitor (if configured) is successful
- The next-hop IP address belongs to one of the outgoing interface subnets

NEW QUESTION 151

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=user, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
     set password xxxxx
   next
end
```

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
#diagnose debug application fnbamd -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 4 for student in WindowsLDAP
opt=27 prot=0
fnbamd_fsm.c[336]_compose _group_list_from_req_Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnband_pop3_start-student
fnbamd_cfg.c[932] fnbamd_cfg-get_ldap_:ist_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[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
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 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the above output, what FortiGate LDAP settings must the administer check? (Choose two.)

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

Answer: BC

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=13141

NEW QUESTION 153
An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit's session to indicate that it has been synchronized to the secondary unit?

A. redir.
B. dirty.
C. synced
D. nds.

Answer: C

Explanation:
The synced sessions have the 'synced' flag. The command 'diag sys session list' can be used to see the sessions on the member, with the associated flags.

NEW QUESTION 158
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# 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=
ha_id=0 policy_dir=0 tunnel=/
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=10.200.1.254/10.0.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.182:80(10.200.1.1:65464
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464(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/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement is correct regarding the output?

A. This session is for HA heartbeat traffic.
B. This session is synced with the slave unit.
C. The inspection of this session has been offloaded to the slave unit.
D. This session cannot be synced with the slave unit.

Answer: B

NEW QUESTION 162
An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

A. Router ID.
B. OSPF interface area.
C. OSPF interface cost.
D. OSPF interface MTU.
E. Interface subnet mask.

Answer: BDE

NEW QUESTION 167
Refer to the exhibit, which shows partial outputs from two routing debug commands.

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

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

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
```

Why is the port2 default route not in the second command output?

A. The port2 interface is disabled in the FortiGate configuration.
B. The port1 default route has a lower distance than the default route using port2.
C. The port1 default route has a higher priority value than the default route using port2.
D. The port1 default route has a lower priority value than the default route using port2.

Answer: B

NEW QUESTION 170
Refer to the exhibit, which contains the output of a debug command.

```
# diagnose hardware sysinfo conserve
memory conserve mode:                on
total RAM:                           3040 MB
memory used:                         2706 MB 89% of total RAM
Memory freeable:                      334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:           2675 MB 88% of total RAM
memory used threshold green:         2492 MB 82% of total RAM
```

If the default settings are in place, what can be concluded about the conserve mode shown in the exhibit?

A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.
B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Answer: C

NEW QUESTION 175
Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # 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
100.64.3.1      4 65501       101     115         0      0    0    never       Active

Total number of neighbors 3
```

What can be concluded 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 BGP session with the local router.
B. The State/PfxRcd for neighbor 100.64.3.1 will not change until an administrator on the local router adjusts the inbound route filtering so that prefixes received can be added to the RIB.
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.

Answer: D

NEW QUESTION 178
Refer to the exhibit, which shows the output of get system ha status. NGFW-1 and NGFW-2 have been up for a week.

```
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: 2021-10-18 12:07:47
Primary selected using:
   <2021/10/18 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
```

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

A. If FGVM...649 is rebooted, FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.

B. If no action is taken, the primary FortiGate will leave the cluster due to the current sync status.
C. If port7 becomes disconnected on the secondary, both FortiGate devices will elect itself the primary.
D. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.

Answer: AC

Explanation:
* A. If FGVM...649 is rebooted, FGVM...650 will become the primary that is normal since it will be the only active firewall and retain that role since override is disabled. Even after FGVM...649 rejoins the cluster, 650 will not fail over as slave. C. If port7 (heartbeat port) becomes disconnected on the secondary, both FortiGate devices will elect itself the primary because when heartbeat communication fails, all cluster members think they are the primary unit (condition referred to as Split Brain) https://docs.fortinet.com/document/fortigate/6.4.0/best-practices/493254/heartbeat-interfaces

NEW QUESTION 180
Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-miltipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

TheBGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

A. Enable the redistribution of connected routers into BGP.
B. Enable the redistribution of static routers into BGP.
C. Disable the setting network-import-check.
D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 185
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 187
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 filler profile.

Answer: C

Explanation:
Example log for no local cache case: #id=93000 msg="pid=57 urlfilter_main-723 in main.c received pkt:count=91 "IPS and WAD will only send request to urlfilter daemon when cache is missed. " So the WAD process by itself found the URL rating in the local cache and didn`t ask for help from the URL process as in the example.

NEW QUESTION 192
An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the
administrator notices that some of the switches in the network continue to send traffic to the former primary device. The administrator decides to enable the setting link-failed-signal to fix the problem.
Which statement about this setting is true?

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

Answer: D

NEW QUESTION 195
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: B

Explanation:
https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt-52/web_proxy.htm#Explicit2
The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

NEW QUESTION 200
An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
B. Redirection of HTTP to HTTPS administrative access is disabled.
C. HTTP administrative access is configured with a port number different than 80.
D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 203
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_EFW-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_EFW-7.0-dumps.html