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

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 2

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 3

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 4

Examine the following partial outputs from two routing debug commands; then answer the question below.
# get router info kernel
tab=254 vf=0 scope=0type=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=0type=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=10.200.2.254 dev=3(port2)
tab=254 vf=0 scope=253type=1 proto=2 prio=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, portl [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3
dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is directly connected, port2
Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!
B. port2.
C. Both portl and port2.
D. port3.

Answer: B

NEW QUESTION 5

An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#     edit 0
#            set gateway 10.20.121.2
#            set priority 20
#            set device "wan1"
#     next
# end
```

Why didn't the script make any changes to the managed device?

A. Commands that start with the # sign are not executed.
B. CLI scripts will add objects only if they are referenced by policies.
C. Incomplete commands are ignored in CLI scripts.
D. Static routes can only be added using TCL scripts.

Answer: A

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc
A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

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
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 8
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 9
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 10
Refer to the exhibit, which contains a TCL script configuration on FortiManager.
An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.

Type	TCL Script ▾
Run script on	Remote FortiGate ... ▾
| Script details | ```
#!
proc do_cmd {cmd} {
puts [exec "$cmd\n" "# " 10]
}
run_cmd "config system interface "
run_cmd "edit port1"
run_cmd "set ip 10.0.1.10 255.255.255.0"
run_cmd "next"
run_cmd "end"
``` |

Why did the TCL script fail to make any changes to the managed device?

A. The TCL command run_cmd has not been created.
B. The TCL script must start with tinclude <>.
C. Incomplete commands are ignored in TCL scripts.
D. Changes to an interface configuration can be made only by a CLI script.

Answer: A

Explanation:
https://docs.fortinet.com/document/fortimanager/7.2.2/administration-guide/914165/tcl-scripts

NEW QUESTION 10
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 11
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 16
Refer to the exhibit, which contains a CLI script configuration on FortiManager.

Script Name	Static Route
Comments	0/255 0/255
Type	CLI Script ▼
Run script on	Remote FortiGate Directly (... ▼
Script details	# conf rout stat # edit 0 # set gateway 10.20.121.2 # set priority 20 # set device "wan1" # next # end

An administrator configured the CLI script on FortiManager, but the script failed to apply any changes to the managed device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two.)

A. Static routes can be added using only TCL scripts.
B. The commands that start with the # sign did not run.
C. CLI scripts must start with #!.
D. Incomplete commands can cause CLI scripts to fail.

Answer: BD

Explanation:
ref CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not "#!" as it is for Tcl scripts.
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

NEW QUESTION 20

Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.

```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session       ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_dst_session      ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_scan             ip=192.168.1.110   dos_id=1  exp=649   pps=0  freq=0
id=udp_flood            ip=192.168.1.110   dos_id=2  exp=653   pps=0  freq=0
id=tcp_src_session      ip=192.168.1.110   dos_id=1  exp=5175  pps=0  freq=8
id=tcp_port_scan        ip=192.168.1.110   dos_id=1  exp=175   pps=0  freq=0
id=ip_src_session       ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=30
id=udp_src_session      ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.
B. Those whose traffic matches an IPS sensor.
C. Those whose traffic exceeded a threshold of a matching DoS policy.
D. Those whose traffic was detected as an anomaly by an IPS sensor.

Answer: A

NEW QUESTION 24
View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: B

NEW QUESTION 25
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 27
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 28
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 31
Refer to the exhibit, which contains 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 unit is zero (0), which statement about the output is true?

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

Answer: C

NEW QUESTION 36
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 37
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
#dia hardware sysinfo shm
SHM counter:           150
SHM allocated:           0
SHM total:       625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:  641236992
SHM FS free:   641208320
SHM FS avail:  641208320
SHM FS alloc:     28672
```

What statement is correct about this FortiGate?

A. It is currently in system conserve mode because of high CPU usage.
B. It is currently in FD conserve mode.
C. It is currently in kernel conserve mode because of high memory usage.
D. It is currently in system conserve mode because of high memory usage.

Answer: D

NEW QUESTION 39
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
        auth:   sha1  edd8141f4956140eef703d9042621d3dbf5cd961
      NPU acceleration: encryption(outbound) decryption(inbound)
```

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

A. The npu_flag for this tunnel is 03.
B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
C. Anti-replay is enabled.
D. The npu_flag for this tunnel is 02.

Answer: AC

NEW QUESTION 44
Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 655
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V   AS        MsgRcvd MsgSent       TblVe
10.200.3.1      4 65501       92       1756          0

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router has a different AS number than the remote peer.
B. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the openConfirm yet.
C. The local router initiated the BGP session to 10.200.3.1 but did not receive a response.
D. The router 10.200.3.1 has authentication configured for BGP and the local router does not.

Answer: C

NEW QUESTION 48
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 52
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 53
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 58
Which statement is true regarding File description (FD) conserve mode?

A. IPS inspection is affected when FortiGate enters FD conserve mode.
B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
C. FD conserve mode affects all daemons running on the device.
D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 62
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. Only the DR receives link state information from non-DR routers.
B. Non-DR and non-BDR routers form full adjacencies to DR only.
C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C

Explanation:
Some special IP multicast addresses are reserved for OSPF: 224.0.0.5: All OSPF routers must be able to transmit and listen to this address. 224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

NEW QUESTION 67
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 69
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 74
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 75
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 79
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 80
Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Preview pending configuration changes for managed devices.
B. Add devices to FortiManager.
C. Import policy packages from managed devices.
D. Install configuration changes to managed devices.
E. Import interface mappings from managed devices.

Answer: AD

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins
There are 4 main wizards:Add Device: is used to add devices to central management and import their configurations.
Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.
Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

NEW QUESTION 81
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 84
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 87
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 91
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 95
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 100
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 102
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 106
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 109
Refer to the exhibit, which contains a TCL script configuration on FortiManager.

Type	TCL Script
Run script on	Remote FortiGate ...

Script details	#!
	proc do_cmd {cmd} {
	puts [exec "$cmd\n" "# " 10]
	}
	run_cmd "config system interface "
	run_cmd "edit port1"
	run_cmd "set ip 10.0.1.10 255.255.255.0"
	run_cmd "next"
	run_cmd "end"

An administrator has configured the TCL script on FortiManager, but failed to apply any changes to the managed device after being executed.
Why did the TCL script fail to make any changes to the managed device?

A. Changes in an interface configuration can only be done by CLI script.
B. The TCL script must start with #include <>.
C. Incomplete commands are ignored in TCL scripts.
D. The TCL command run_cmd has not been created.

Answer: D

NEW QUESTION 113
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# 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 7 sent 9
    LS-Req received 2 sent 2, LS-Upd received 7 sent 5
    LS-Ack received 4 sent 3, Discarded 1
```

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

A. In the network on port4, two OSPF routers are down.
B. Port4 is connected to the OSPF backbone area.
C. The local FortiGate's OSPF router ID is 0.0.0.4
D. The local FortiGate has been elected as the OSPF backup designated router.

Answer: BC

NEW QUESTION 116
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 117
A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fsso list' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

A. The user student must not be listed in the CA's ignore user list.
B. The user student must belong to one or more of the monitored user groups.
C. The student workstation's IP subnet must be listed in the CA's trusted list.
D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Answer: AD

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

NEW QUESTION 119
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # diagnose 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 tun_id=10.200.4.1 dst_mtu=1500 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev
frag-rfc  accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/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=2
   src: 0:10.1.2.0/255.255.255.0:0
   dst: 0:10.1.1.0/255.255.255.0:0
   SA:  ref=3 options=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
        seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
   life: type=01 bytes=0/0 timeout=42900/43200
   dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
        ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
   enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
        ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
   dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. The remote gateway has quick mode selectors containing a destination subnet of 10.1.2.0/24.
B. The remote gateway IP is 10.200.5.1.
C. DPD is disabled.
D. Anti-replay is enabled.

Answer: AD

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 427, 444
Since the local subnet is 10.1.2.0/24, the remote gateway has the destination subnet as 10.1.2.0. The remote gateway IP is 10.200.4.1. DPD is enabled (dpd-link=on)

NEW QUESTION 120
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 124
Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. OSPF interface network types match.
B. OSPF router IDs are unique.
C. OSPF interface priority settings are unique.
D. Authentication settings match.
E. OSPF link costs match.

Answer: ABD

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 280

NEW QUESTION 126
View the exhibit, which contains the output of a BGP debug command, and 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 of the following statements about the exhibit are true? (Choose two.)

A. For the peer 10.125.0.60, the BGP state of is Established.
B. The local BGP peer has received a total of three BGP prefixes.
C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: AD

NEW QUESTION 131
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 136
Which statement about memory conserve mode is true?

A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: D

NEW QUESTION 139
Refer to exhibit, which contains the output of a BGP debug command.


```
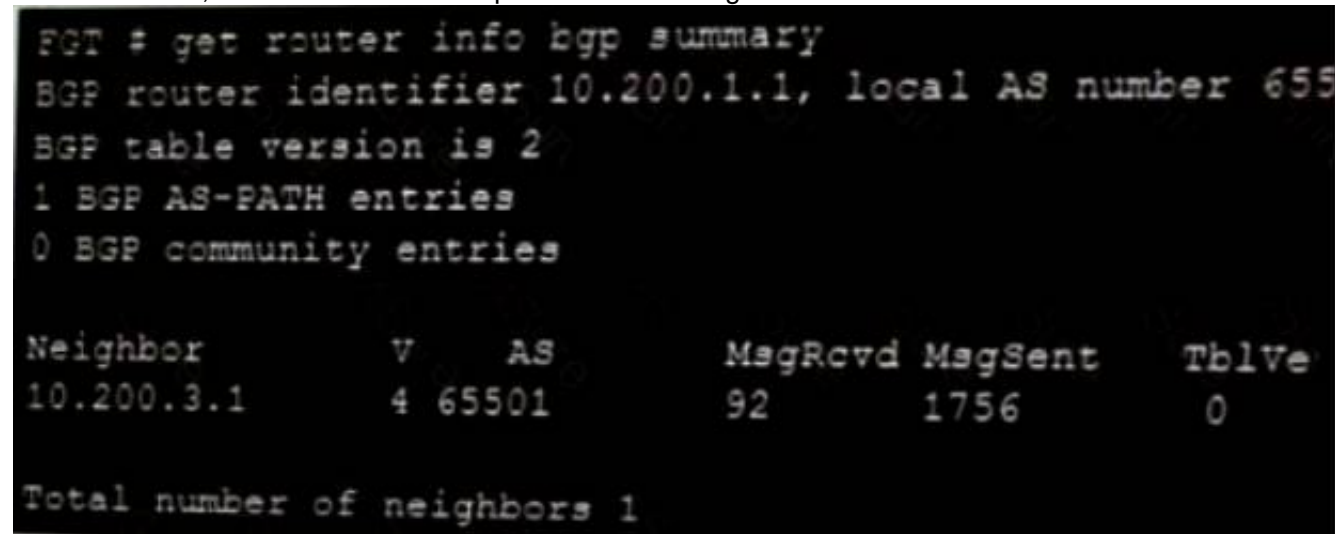FGT # get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 655
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor         V    AS         MsgRcvd MsgSent     TblVe
10.200.3.1       4 65501        92      1756        0

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
B. The TCP session to 10.200.3.1 has not completed the three-way handshake.
C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:
BGP neighbor states and how they change:• Idle: Initial state• Connect: Waiting for a successful three-way TCP connection• Active: Unable to establish the TCP session• OpenSent: Waiting for an OPEN message from the peer• OpenConfirm: Waiting for the keepalive message from the peer• Established: Peers have successfully exchanged OPEN and keepalive messages

NEW QUESTION 141
View the exhibit, which contains the output of a web diagnose command, and then answer the question below.

```
# diagnose webfilter fortiguard statistics list           # diagnose webfilter fortiguard statistics list

Raring Statistics:                                          Cache Statistics:
=============================                               =======================
DNS filures                    :     273                    Maximum memory          :     0
DNS lookups                    :     280                    Memory usage            :     0
Data send failures             :       0
Data read failures             :       0                    Nodes                   :     0
Wrong package type             :       0                      Leaves                :     0
Hash table miss                :       0                      Prefix nodes          :     0
Unknown server                 :       0                      Exact nodes           :     0
Incorrect CRC                  :       0
Proxy requests failures        :       0                    Requests                :     0
Request timeout                :       1                    Misses                  :     0
Total requests                 :    2409                    Hits                    :     0
Requests to FortiGuard servers :    1182                      Prefix hits           :     0
Server errored responses       :       0                      Exact hits            :     0
Relayed rating                 :       0
Invalid profile                :       0                    No cache directives     :     0
                                                            Add after prefix        :     0
Allowed                        :    1021                    Invalid DB put          :     0
Blocked                        :    3909                    DB updates              :     0
Logged                         :    3927
Blocked Errors                 :     565                    Percent full            :    0%
Allowed Errors                 :       0                      Branches              :    0%
Monitors                       :       0                      Leaves                :    0%
Authenticates                  :       0                        Prefix nodes        :    0%
Warnings                       :      18                        Exact nodes         :    0%
Ovrd request timeout           :       0
Ovrd send failures             :       0                    Miss rate               :    0%
Ovrd read failures             :       0                    Hit rate                :    0%
Ovrd errored responses         :       0                      Prefix hits           :    0%
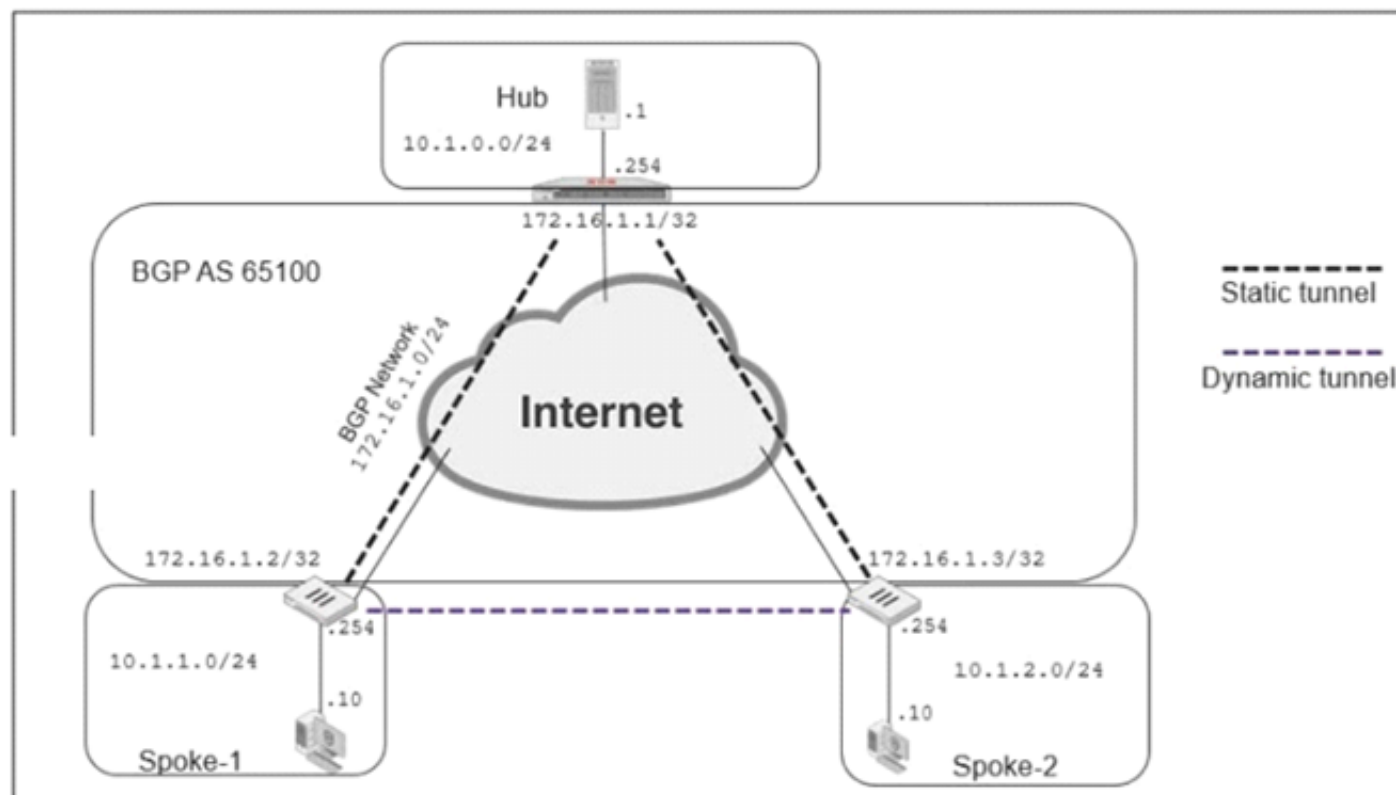...                                                           Exact hits            :    0%
```

Which one of the following statements explains why the cache statistics are all zeros?

A. The administrator has reallocated the cache memory to a separate process.
B. There are no users making web requests.
C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Answer: C

NEW QUESTION 144
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 149
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 150
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 152
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 154
Refer to the exhibit, which shows the output of a debug command.

```
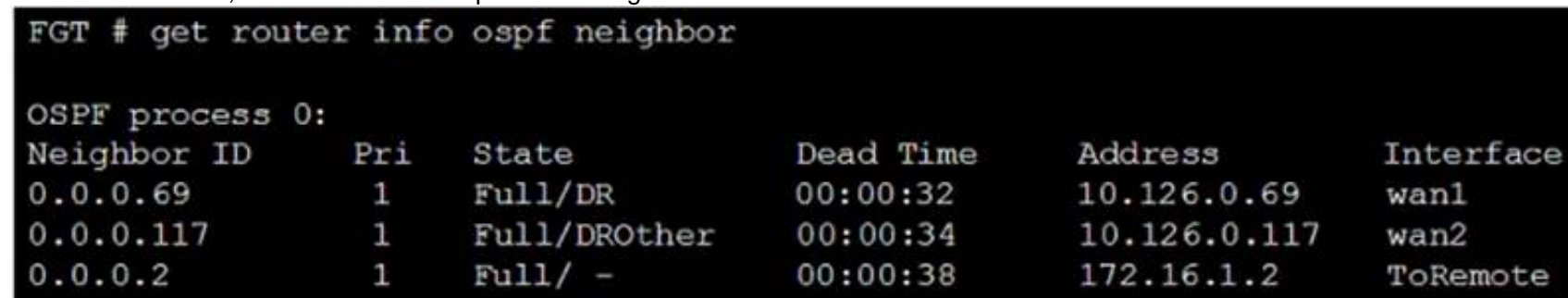FGT # get router info ospf neighbor

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 158
What is the diagnose test application ipsmonitor 99 command used for?

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

Answer: D

NEW QUESTION 159
In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

A. It provides VM license validation services.
B. It supports rating requests from non-FortiGate devices.
C. It caches available firmware updates for unmanaged devices.
D. It can be configured as an update server, a rating server, or both.

Answer: AD

NEW QUESTION 163
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 168
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 172
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 174
An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMSs in FortiManager.
How should the administrator accomplish this task?

A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.
B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.
C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.
D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 244

NEW QUESTION 179
What is the purpose of an internal segmentation firewall (ISFW)?

A. It inspects incoming traffic to protect services in the corporate DMZ.
B. It is the first line of defense at the network perimeter.
C. It splits the network into multiple security segments to minimize the impact of breaches.
D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

Answer: C

Explanation:
ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

NEW QUESTION 184
Which two conditions would prevent a static route from being added to the routing table? (Choose two.)

A. There is another other route to the same destination, with a lower distance.
B. The route has a lower priority value than another route to the same destination.
C. The next-hop IP address is unreachable.
D. The interface specified in the route configuration is down

Answer: AD

Explanation:
The routing table contains only the static route with the lowest distance https://community.fortinet.com/t5/FortiGate/Technical-Note-Routing-behavior-depending-on-distance-and/ta-p/

NEW QUESTION 187
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 189
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 191
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 192

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 196
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 197
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 be concluded about the debug output in this scenario?

A. Servers with a negative TZ value are less preferred for rating requests.
B. There is a natural correlation between the value in the Packets field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

Answer: B

NEW QUESTION 198
A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-d ns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878   n_dns_fails= 2   n_dns_timeout=875
n_dns_success=0

n_snd_retries=0   n_snd_fails=0  n_snd_success=0  n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

A. The connectivity between the FortiGate unit and the DNS server.
B. The connectivity between the client workstations and the DNS server.
C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

NEW QUESTION 202
In which two states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting for FIN ACK
B. A UDP session with packets sent and received
C. A UDP session with only one packet received
D. A TCP session waiting for the SYN ACK

Answer: CD

NEW QUESTION 204
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 205
Which two tasks are automated using the Import Configuration wizard on FortiManager? (Choose two.)

A. Importing firewall address objects from managed devices
B. Importing interface mappings from managed devices
C. Importing static and dynamic route configurations from managed devices
D. Importing devices to FortiManager

Answer: AB

Explanation:
https://docs.fortinet.com/document/fortimanager/7.0.5/administration-guide/337348

NEW QUESTION 209
Which of the following statements are correct regarding application layer test commands? (Choose two.)

A. They are used to filter real-time debugs.
B. They display real-time application debugs.
C. Some of them display statistics and configuration information about a feature or process.
D. Some of them can be used to restart an application.

Answer: CD

Explanation:
Application layer test commands don't display info in real time, but they do show statistics and configuration info about a feature or process. You can also use some of these commands to restart a process or execute a change in its operation.

NEW QUESTION 211
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 216
......

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