NSE7_EFW-6.2^Q&As^

Fortinet NSE 7 - Enterprise Firewall 6.2

QUESTION 1

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 user. This limit CANNOT be modified by the administrator.

B. FortiGate limits the total number of simultaneous explicit web proxy users.

C. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator

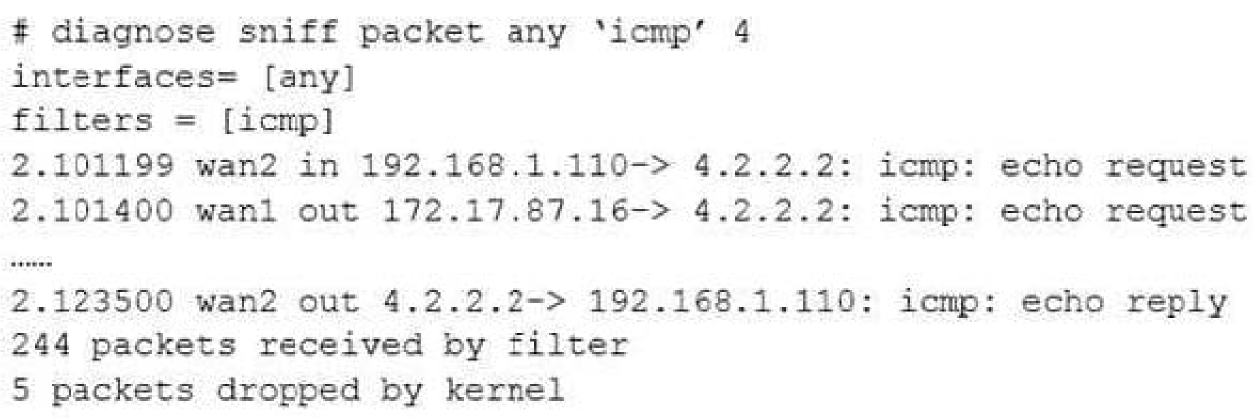
D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: B

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.

QUESTION 2

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.

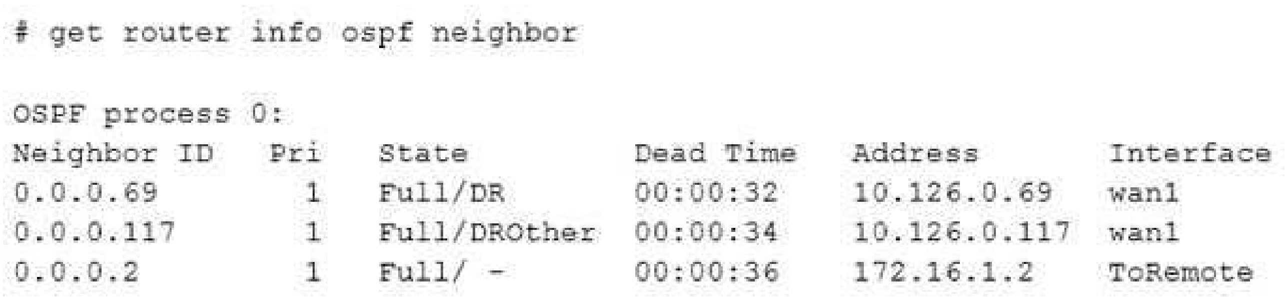
D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Correct Answer: D

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

QUESTION 3

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.)

A. The interface ToRemote is OSPF network type point-to-point.

B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.

C. The local FortiGate is the backup designated router for the wan1 network.

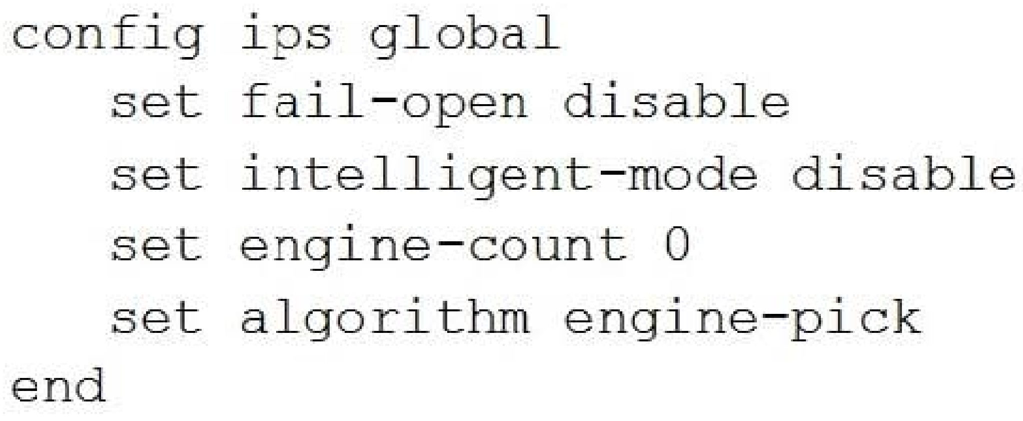
D. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.

Correct Answer: AC

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

QUESTION 4

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.

Correct Answer: A

QUESTION 5

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.

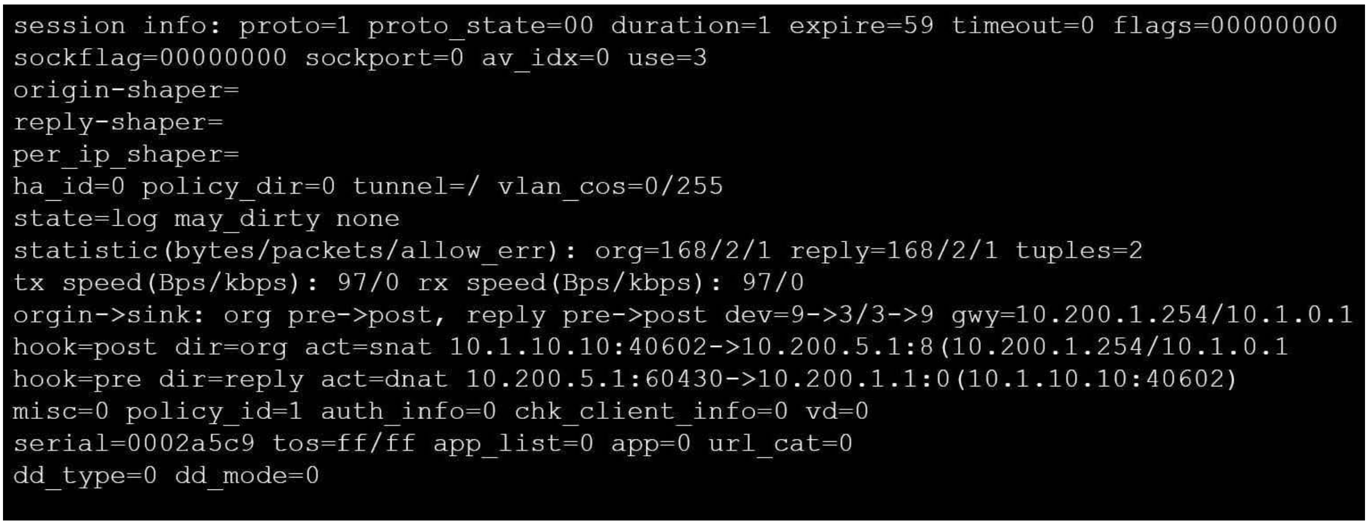
D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Correct Answer: C

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

QUESTION 6

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
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
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.

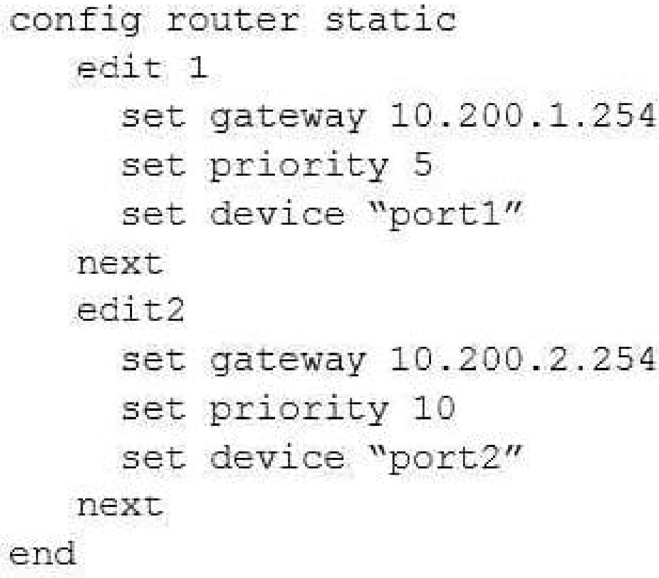
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.

D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

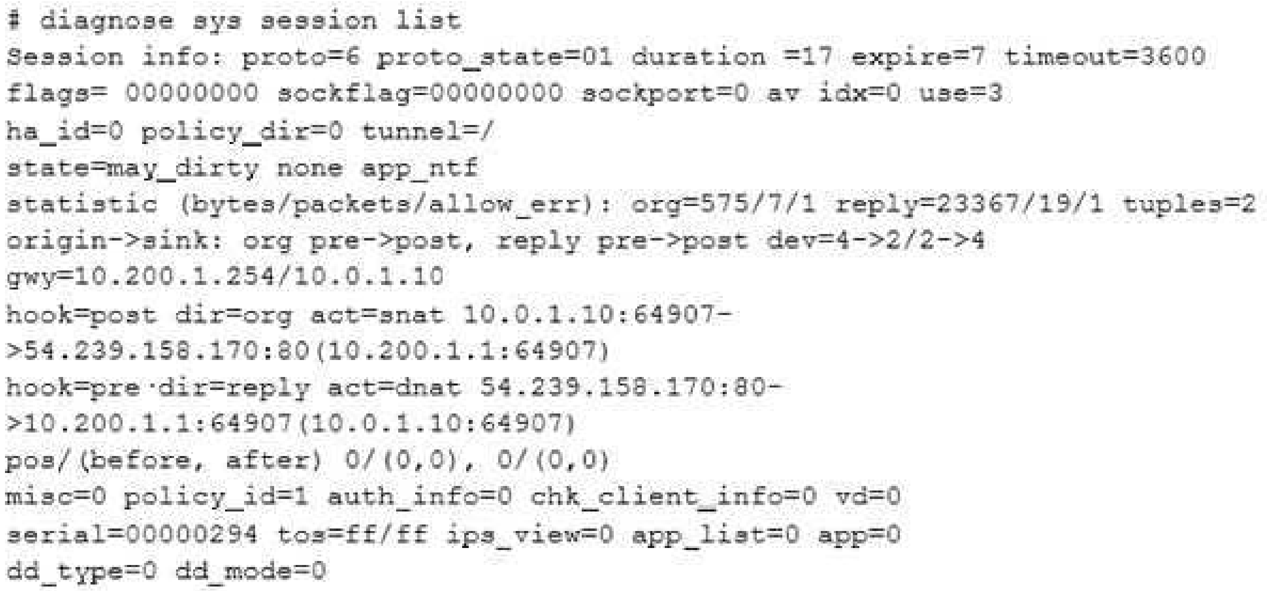
Correct Answer: B

QUESTION 7

A FortiGate has two default routes: All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:



```
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device "port1"
   next
   edit2
      set gateway 10.200.2.254
      set priority 10
      set device "port2"
   next
end
```



```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

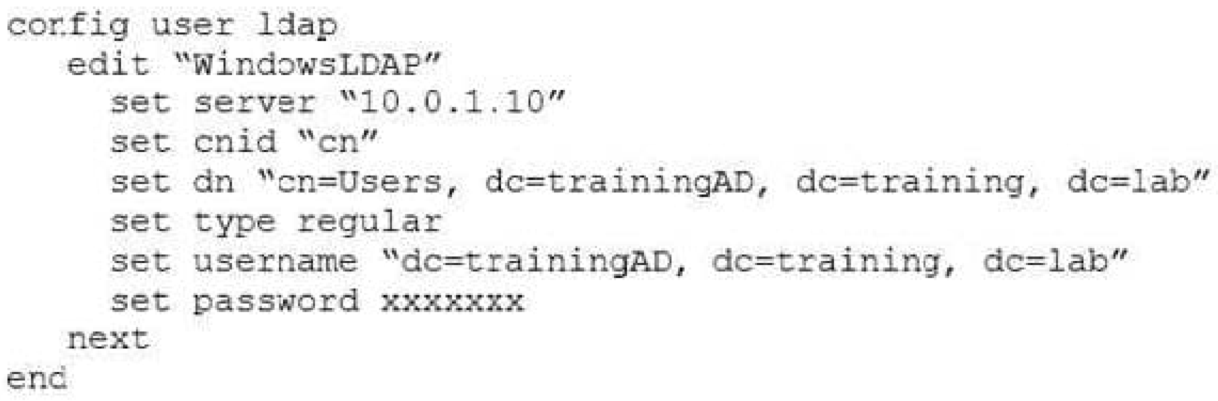
C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A

QUESTION 8

A FortiGate device has the following LDAP configuration:



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

The administrator executed the `dsquery\\' command in the Windows LDAp server 10.0.1.10, and got the following output: >dsquery user -samid administrator "CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab"

Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.

B. username.

C. password.

D. dn.

Correct Answer: B

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

QUESTION 9

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.

Correct Answer: B

QUESTION 10

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.

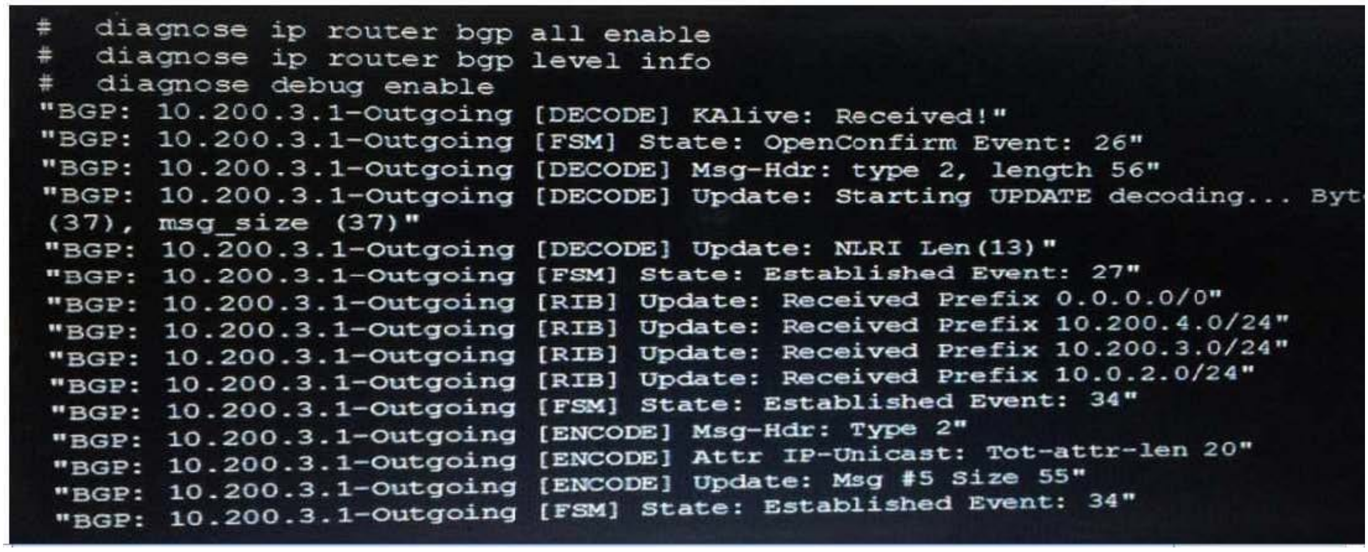
D. At least one of the student\\'s user groups must be allowed by a FortiGate firewall policy.

Correct Answer: AD

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

QUESTION 11

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below: Which statements are true regarding the output in the exhibit? (Choose two.)



```
#  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"
```

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.

Correct Answer: AB

QUESTION 12

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

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Correct Answer: BD

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.

QUESTION 13

An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2

What information is included in the output of the sniffer? (Choose two.)

A. Ethernet headers.

B. IP payload.

C. IP headers.

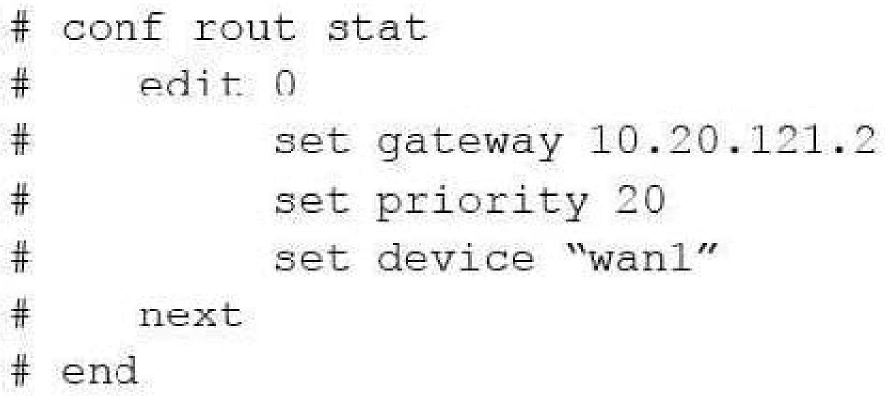
D. Port names.

Correct Answer: BC

https://kb.fortinet.com/kb/documentLink.do?externalID=11186

QUESTION 14

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.

Correct Answer: A

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Scripts/1000_Script%20samples/02 00_CLI%20scripts+.htm#Error_Messages 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.

QUESTION 15

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.

Correct Answer: CDE

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