Practice Exam Questions

FORTINET

NSE7_EFW-7.0

Fortinet NSE 7

Enterprise Firewall 7.0

EXAMKILLER

Help Pass Your Exam At First Try

Fortinet

Exam NSE7_EFW-7.0

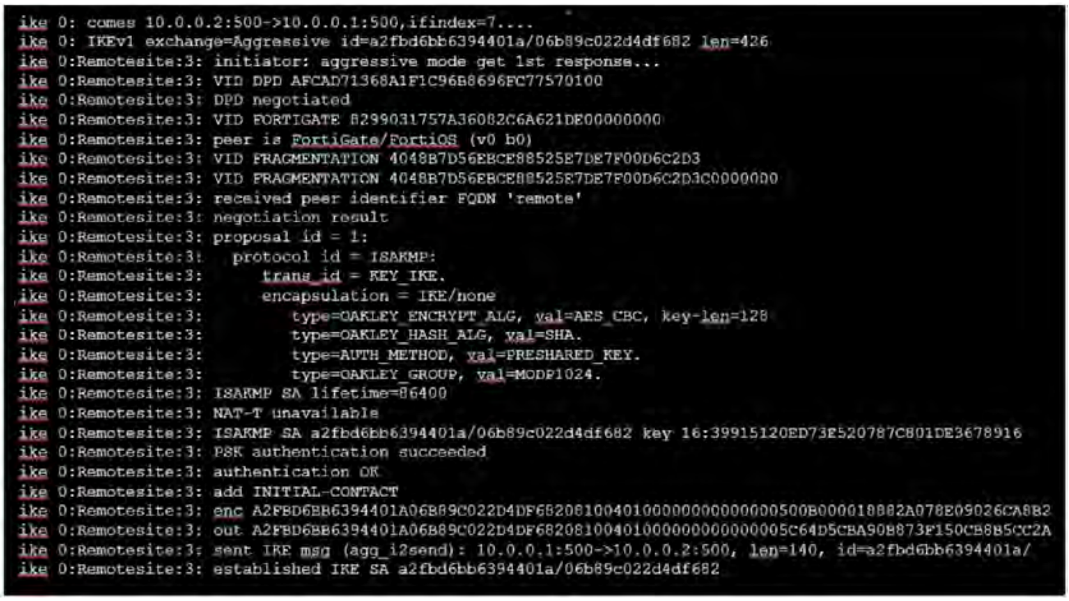
Fortinet NSE 7 - Enterprise Firewall 7.0

Version: 4.0

[Total Questions: 163]

Question No : 1

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



```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7....
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0:Remotesite:3: initiator: aggressive mode get 1st response...
ike 0:Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:Remotesite:3: DPD negotiated
ike 0:Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0:Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:Remotesite:3: received peer identifier FQDN 'remote'
ike 0:Remotesite:3: negotiation result
ike 0:Remotesite:3: proposal id = 1:
ike 0:Remotesite:3:   protocol id = ISAKMP:
ike 0:Remotesite:3:      trans_id = KEY_IKE.
ike 0:Remotesite:3:      encapsulation = IKE/none
ike 0:Remotesite:3:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:Remotesite:3:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:Remotesite:3:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:Remotesite:3:         type=OAKLEY_GROUP, val=MODP1024.
ike 0:Remotesite:3: ISAKMP SA lifetime=86400
ike 0:Remotesite:3: NAT-T unavailable
ike 0:Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0:Remotesite:3: PSK authentication succeeded
ike 0:Remotesite:3: authentication OK
ike 0:Remotesite:3: add INITIAL-CONTACT
ike 0:Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A078E09026CA8B2
ike 0:Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0:Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0:Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

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

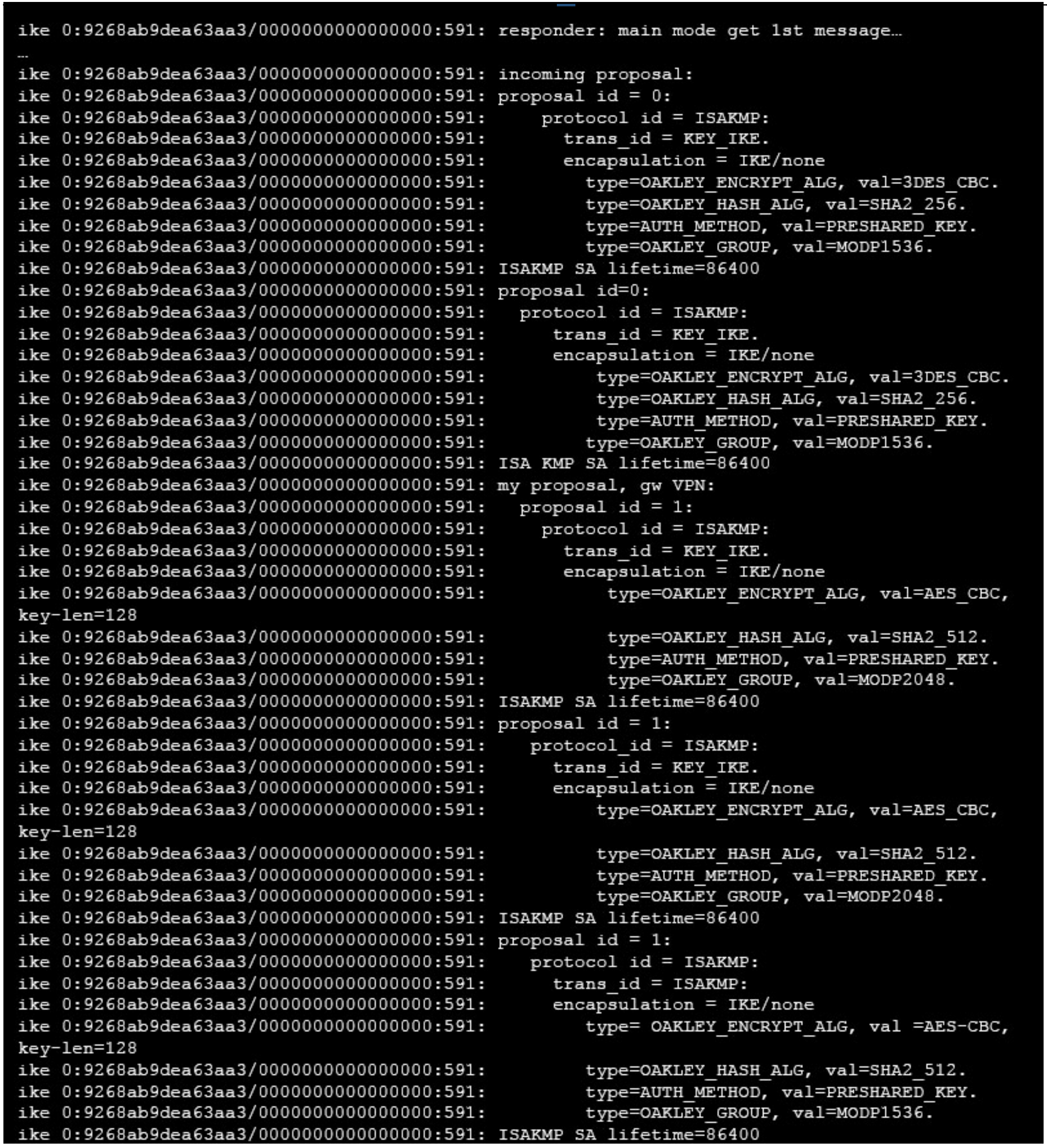
A. The initiator provided remote as its IPsec peer ID.
B. It shows a phase 2 negotiation.
C. Perfect Forward Secrecy (PFS) is enabled in the configuration.
D. The local gateway IP address is 10.0.0.1.

Answer: A,D

Explanation: A because : received peer identifier FQDN 'remote' D because : ike 0: comes 10.0.0.2:500 -> 10.0.0.1:500

Question No : 2

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

Question No : 3

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 initially. The interfaces will be automatically generated after the administrator configures all of the required settings.
C. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.
D. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

Answer: A

Explanation: 1- Create a VPN Community

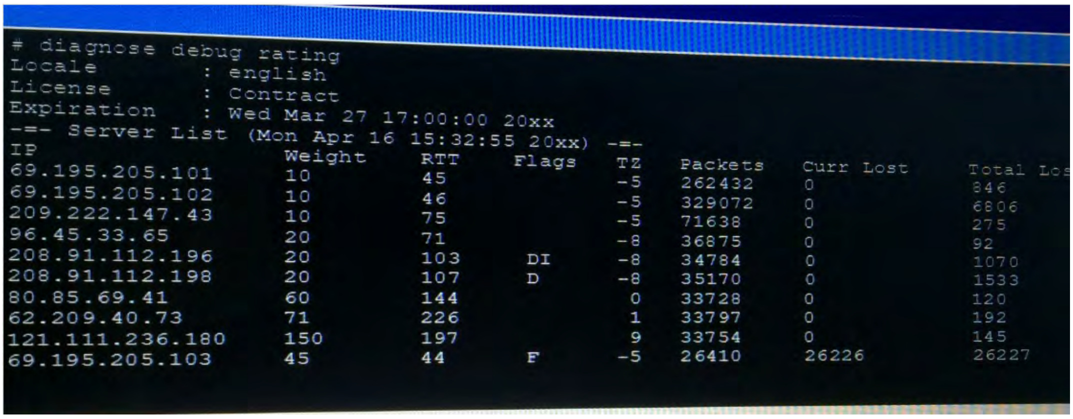
2- Install VPN Configuration

3- Add IPsec Firewall Policies

4- Install the Policies

Question No : 4

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



```
# diagnose debug rating
Locale          : english
License         : Contract
Expiration      : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP
                   Weight     RTT     Flags    TZ   Packets   Curr Lost     Total Los
69.195.205.101     10         45               -5   262432    0             846
69.195.205.102     10         46               -5   329072    0             6806
209.222.147.43     10         75               -5   71638     0             275
96.45.33.65        20         71               -8   36875     0             92
208.91.112.196     20         103      DI      -8   34784     0             1070
208.91.112.198     20         107      D       -8   35170     0             1533
80.85.69.41        60         144               0   33728     0             120
62.209.40.73       71         226               1   33797     0             192
121.111.236.180    150        197               9   33754     0             145
69.195.205.103     45         44       F       -5   26410     26226         26227
```

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

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

Answer: B,C

Question No : 5

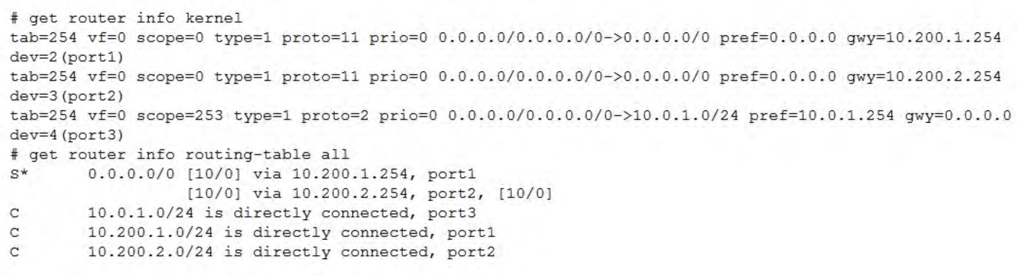
How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

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

Answer: A

Question No : 6

View these partial outputs from two routing debug commands:



```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```

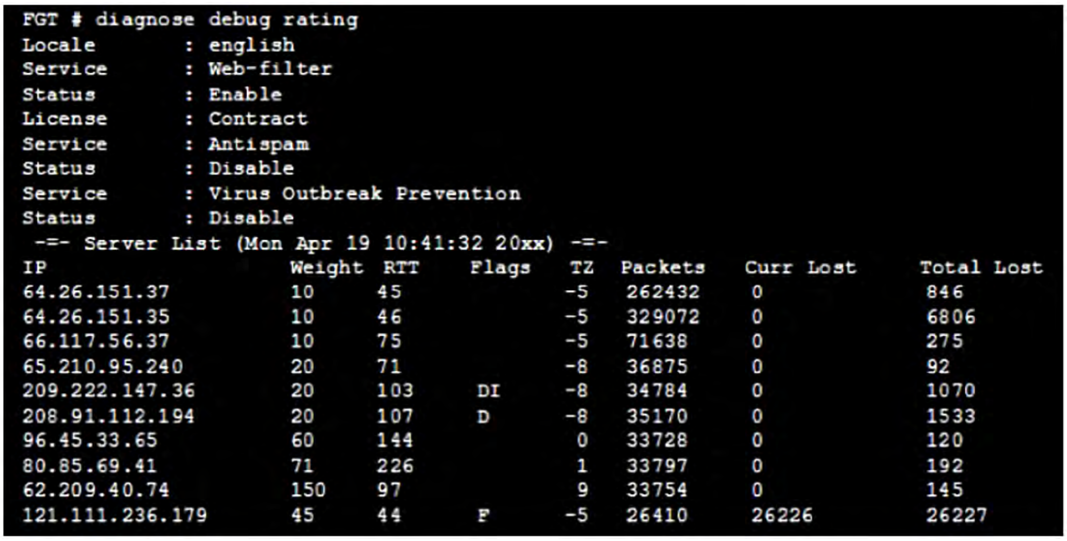
Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

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

Answer: C

Question No : 7

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

Question No : 8

An administrator has configured two FortiGate devices for an HA cluster. While testing the

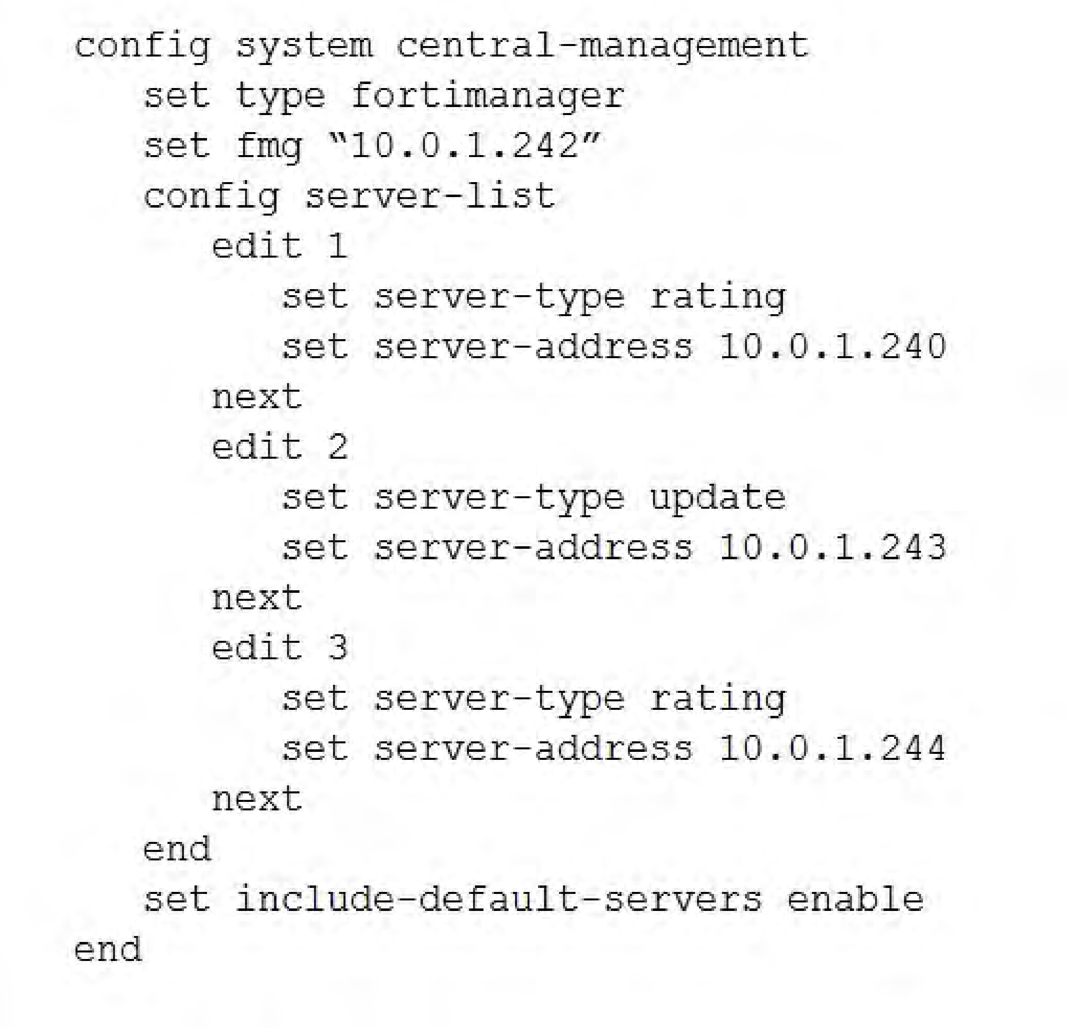
HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

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

Question No : 9

View the central management configuration shown in the exhibit, and then answer the question below.



```
config system central-management
   set type fortimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
         set server-type update
         set server-address 10.0.1.243
      next
      edit 3
         set server-type rating
         set server-address 10.0.1.244
      next
   end
   set include-default-servers enable
end
```

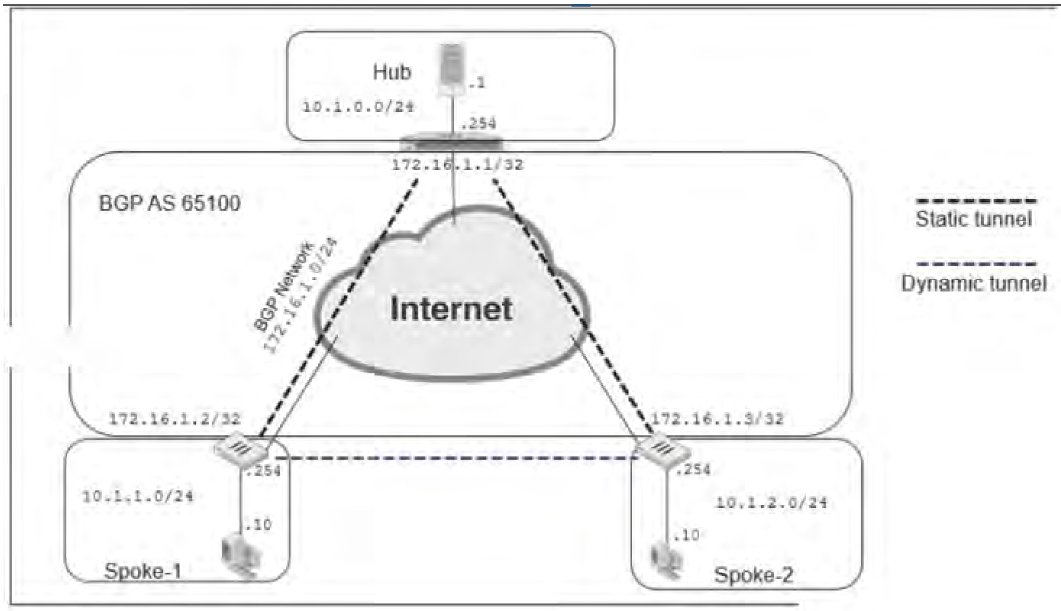
Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

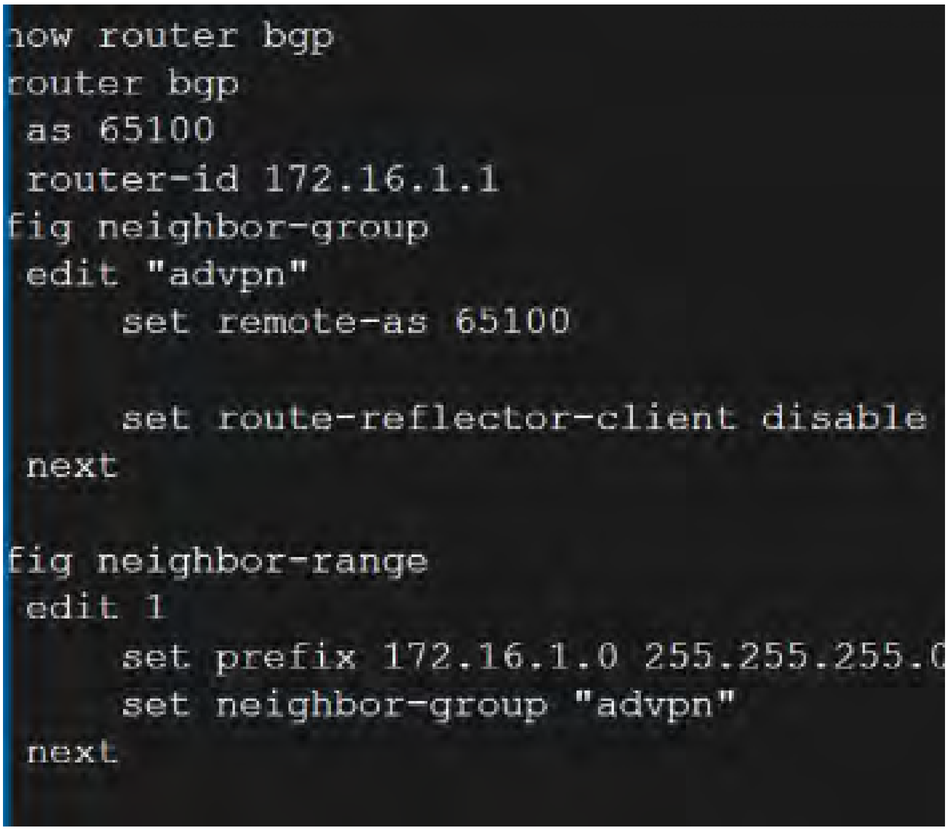
A. 10.0.1.240
B. One of the public FortiGuard distribution servers
C. 10.0.1.244
D. 10.0.1.242

Answer: B

Question No : 10

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?

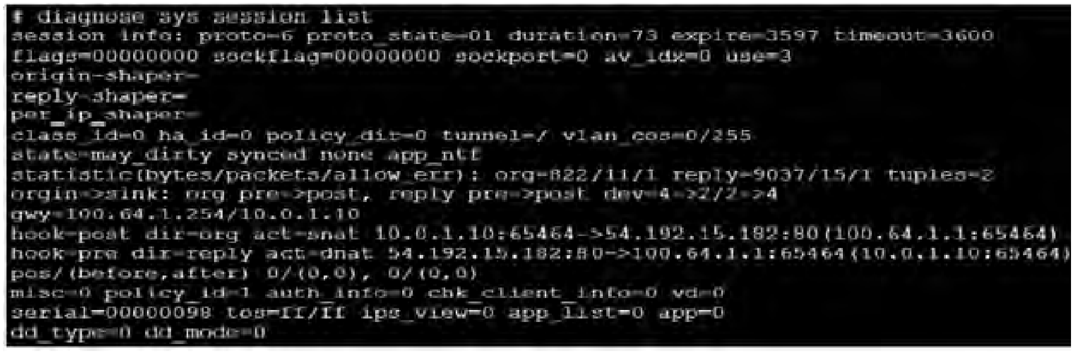
A. Configure an individual neighbor and remove neighbor-range configuration.
B. Configure the hub as a route reflector client.
C. Change the router id to 10.1.0.254.
D. Make the configuration of remote-as different from the configuration of local-as.

Answer: B

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

Question No : 11

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
```

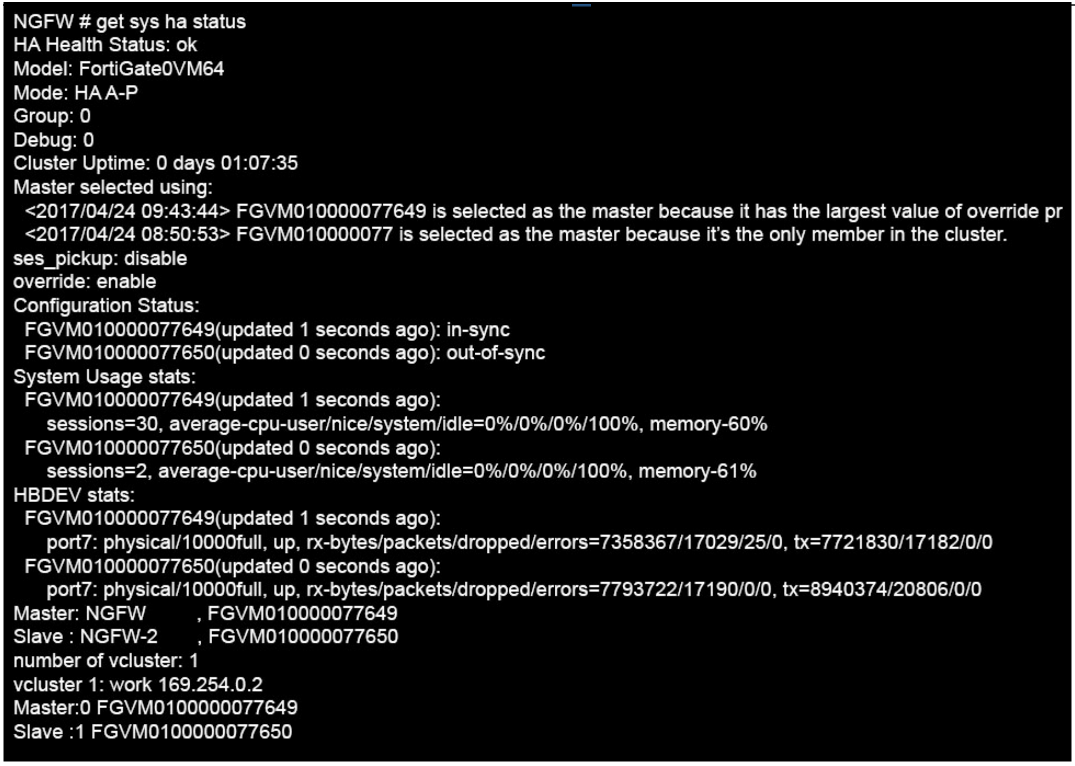
If the HA ID for the primary unit is zero (0), which statement about the output is true?

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

Question No : 12

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: A,D

Question No : 13

Which statement about protocol options is true?

A. Protocol options allows administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
B. Protocol options allows administrators the ability to configure the Any setting for all enabled protocols which provides the most efficient use of system resources.
C. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
D. Protocol options allows administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

Answer: D

Question No : 14

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.
B. TCP half close.
C. TCP time wait.
D. TCP session time to live.

Answer: A

Explanation:

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html

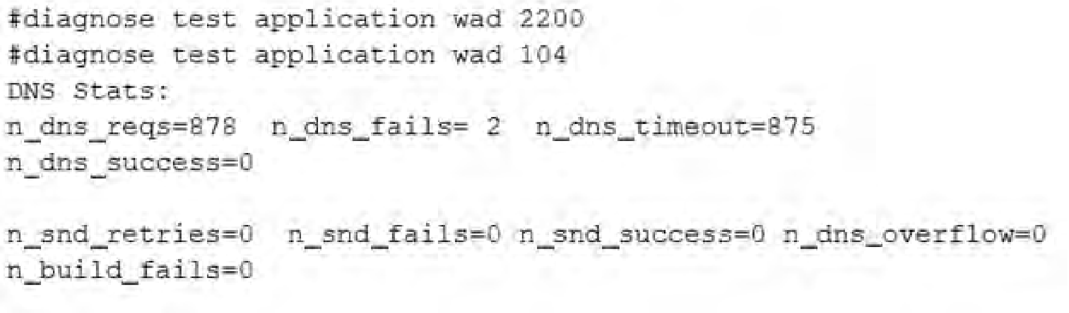
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACKremains in the table.

The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACKremains in the table.

The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in thetable. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

Question No : 15

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-dns-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
```

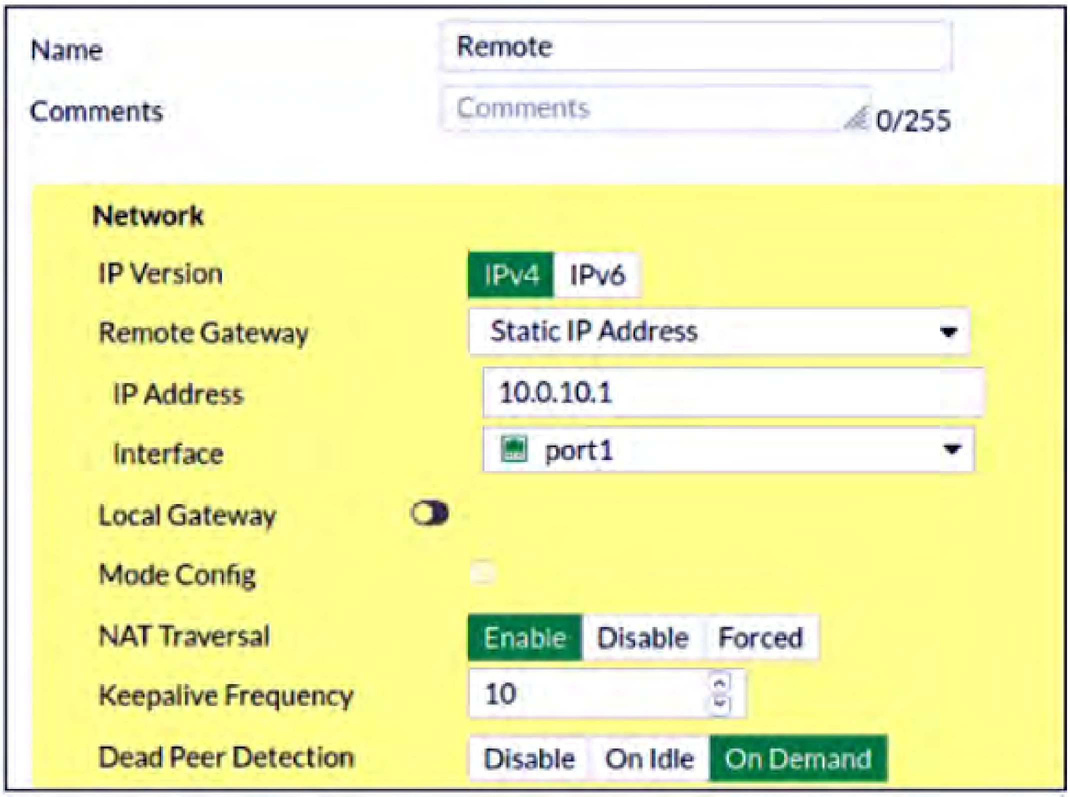
What should the administrator check to fix the problem?

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

Question No : 16

Refer to the exhibit, which contains a screenshot of some phase 1 settings.



Name	Remote
Comments	Comments 0/255
Network	
IP Version	[✓ IPv4] IPv6
Remote Gateway	Static IP Address
IP Address	10.0.10.1
Interface	port1
Local Gateway	○
Mode Config	□
NAT Traversal	[✓ Enable] Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable On Idle [✓ On Demand]

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1

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

A. The administrator must also run the command diagnose debug enable.
B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.
C. The log-filter setting is incorrect. The VPN traffic does not match this filter.
D. The debug shows only error messages. If there is no output, then the phase 1 and phase 2 configurations match.

Answer: A

Explanation: https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPSec-VPN-Diagnostics-Possible-reasons/ta-p/192006

Question No : 17

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: A,D

Reference: https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/668612/using-the-install-wizard-to-install-device-settings-only

Question No : 18

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