Vendor: Fortinet

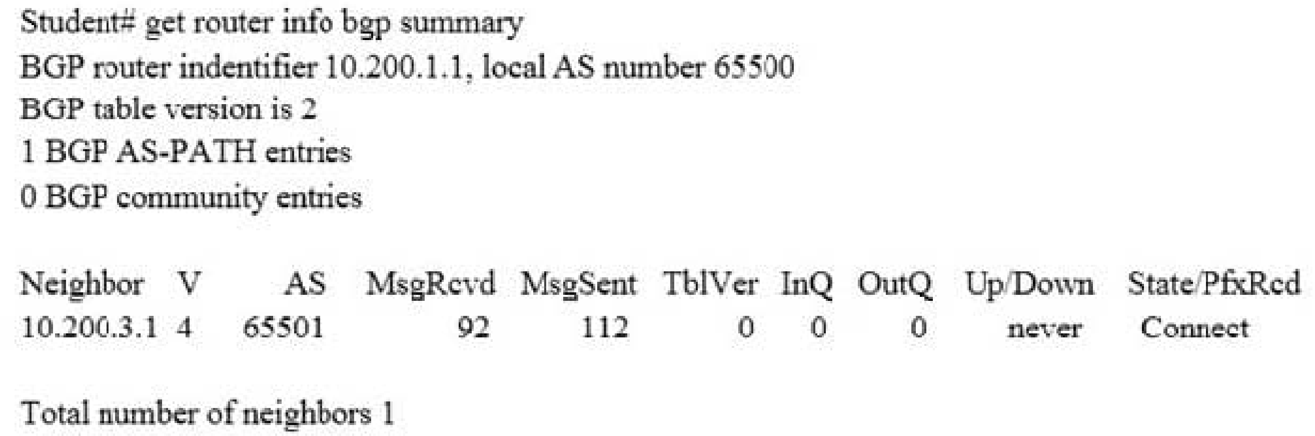
Exam Code:NSE7

Exam Name: Fortinet Troubleshooting Professional

Version: Demo

QUESTION 1

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.

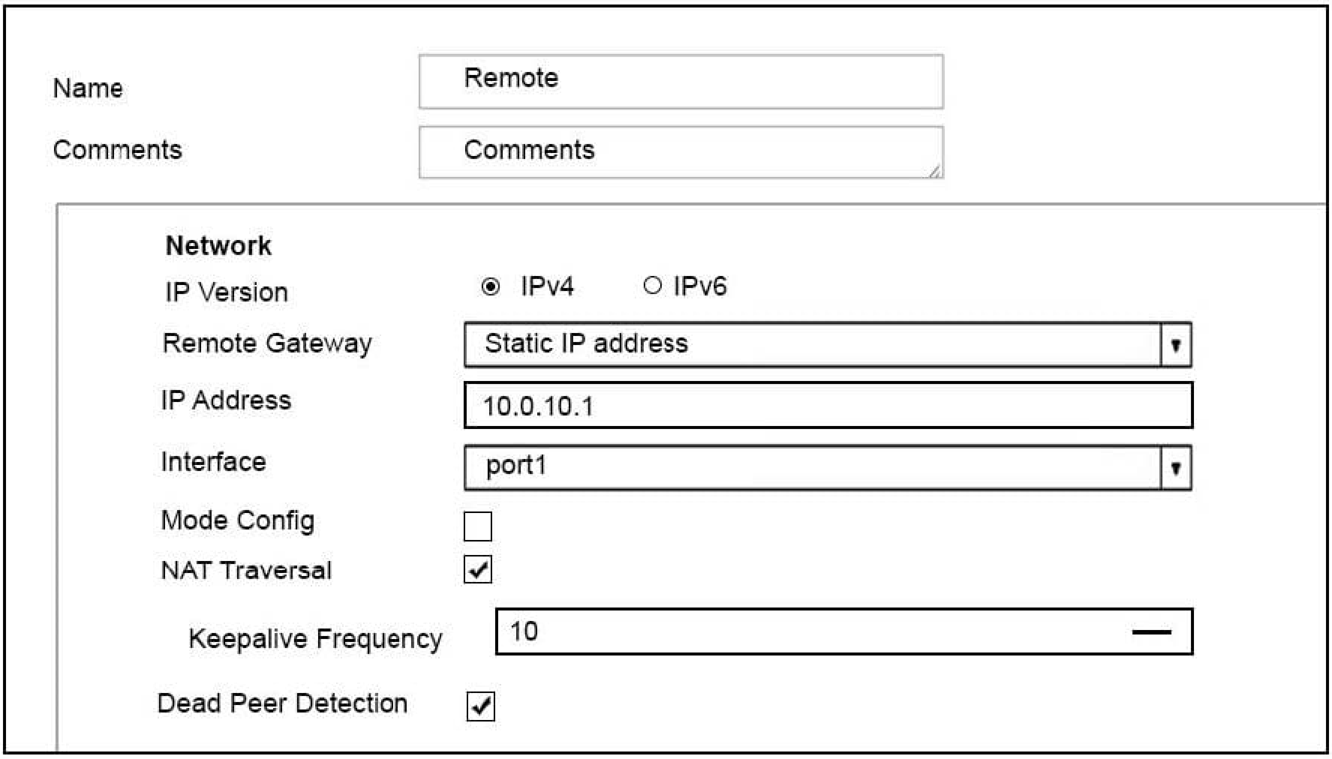
C. The local peer has received the BGP prefixed from the remote peer.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Correct Answer: B

QUESTION 2

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

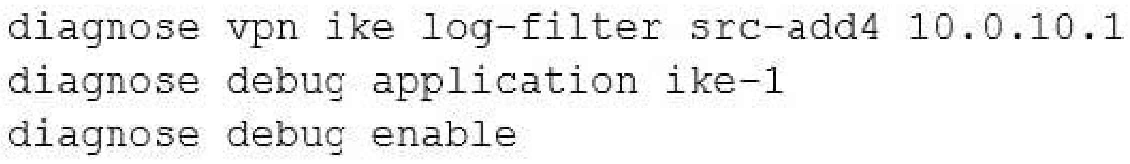


Name	Remote
Comments	Comments

Network

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

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



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

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

A. The debug output shows phases 1 and 2 negotiations only. Once the tunnel is up, it does not show any more output.

B. The log-filter setting was set incorrectly. The VPN\\'s traffic does not match this filter.

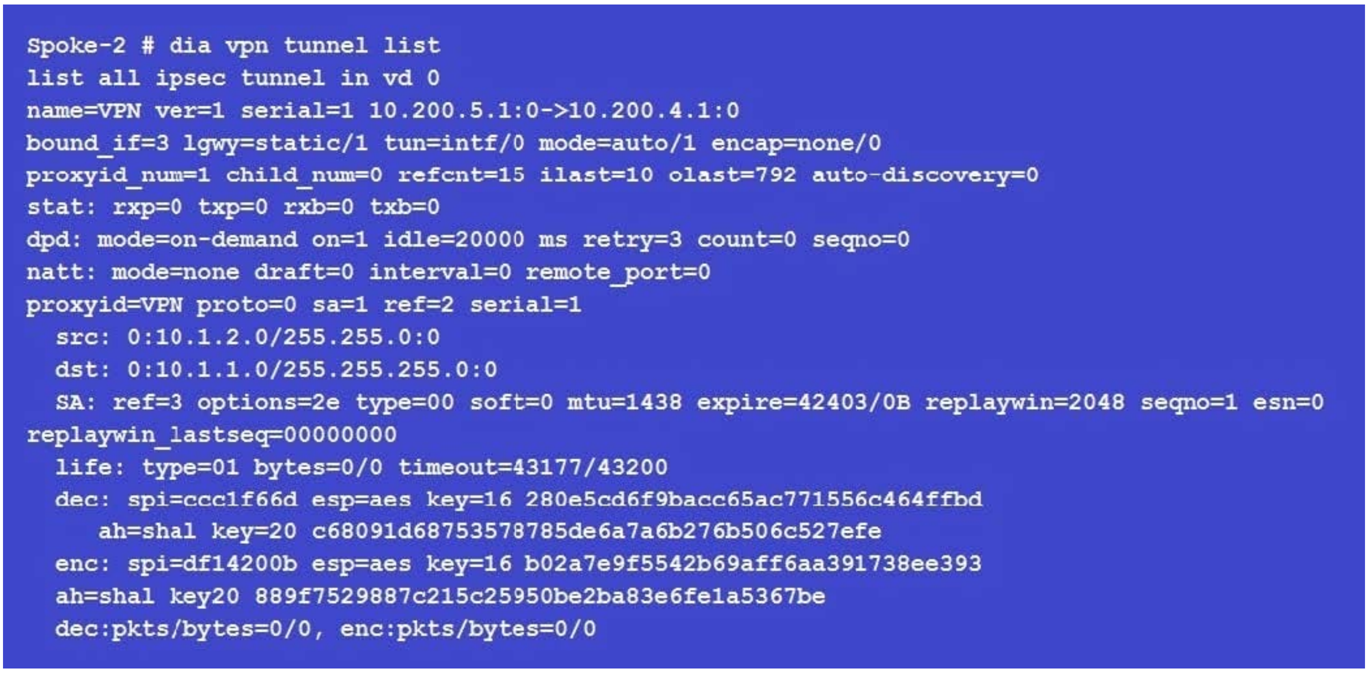
C. The debug shows only error messages. If there is no output, then the tunnel is operating normally.

D. The debug output shows phase 1 negotiation only. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Correct Answer: D

QUESTION 3

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



```
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=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms 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: 0:10.1.2.0/255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
     ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=sha1 key20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which of the following statements is correct?

A. Anti-reply is enabled.

B. DPD is disabled.

C. Quick mode selectors are disabled.

D. Remote gateway IP is 10.200.5.1.

Correct Answer: A

QUESTION 4

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.

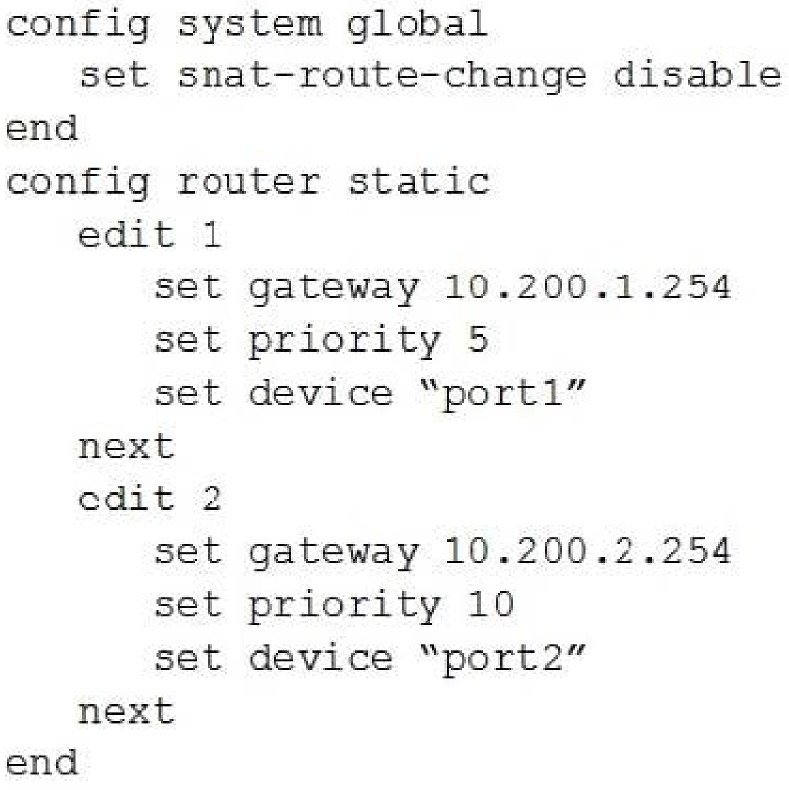
C. The student workstation\\'s IP subnet must be listed in the CA\\'s trusted list.

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

Correct Answer: BD

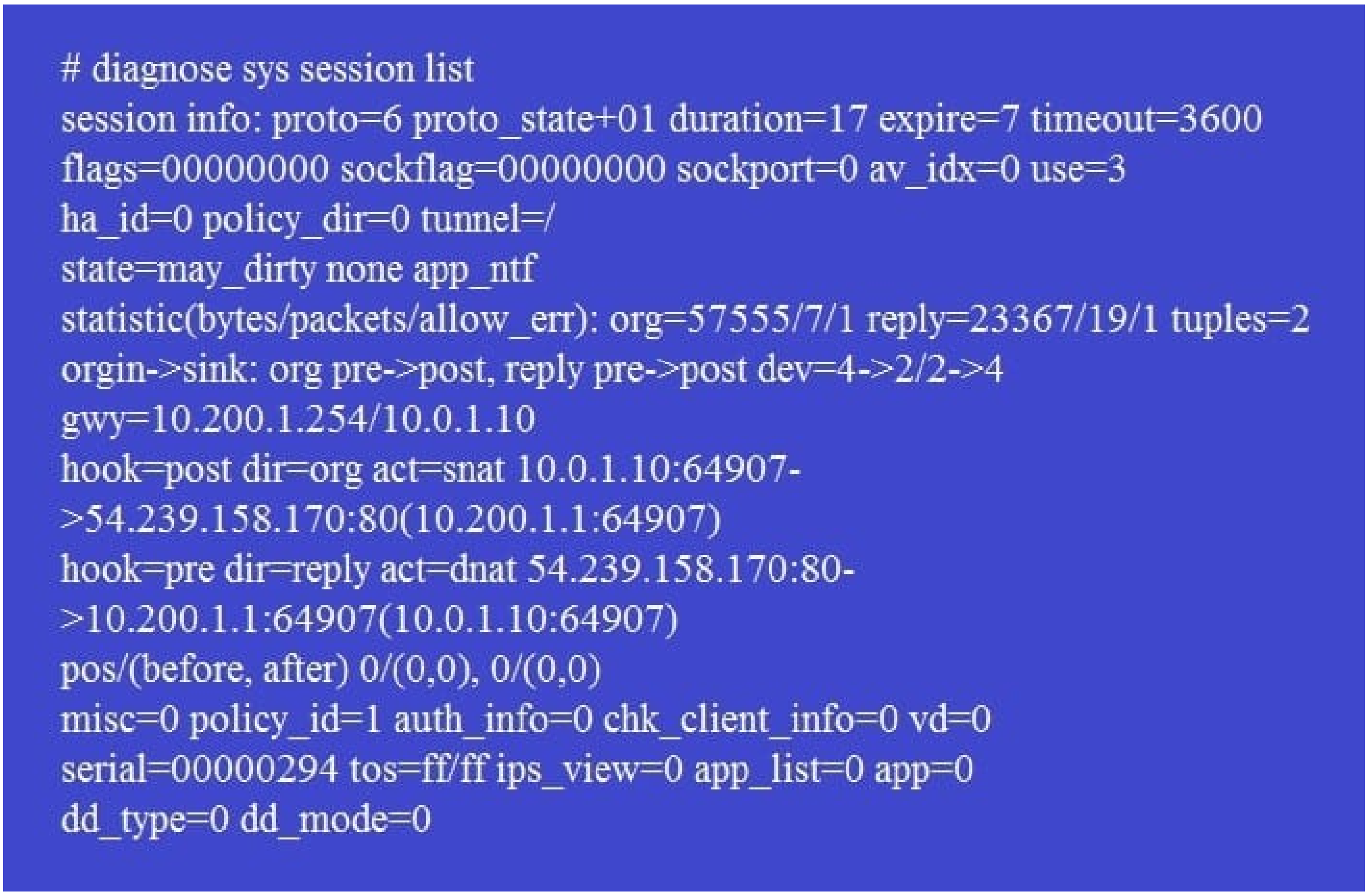
QUESTION 5

View the following FortiGate configuration.



```
config system global
   set snat-route-change disable
end
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device “port1”
   next
   cdit 2
      set gateway 10.200.2.254
      set priority 10
      set device “port2”
   next
end
```

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network:



```
# 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=57555/7/1 reply=23367/19/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=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
```

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user\\'s session?

A. The session would remain in the session table, and its traffic would still egress from port1.

B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

C. The session would remain in the session table, and its traffic would start to egress from port2.

D. The session would be deleted, so the client would need to start a new session.

Correct Answer: D

QUESTION 6

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

A. redir.

B. dirty.

C. synced

D. nds.

Correct Answer: C

QUESTION 7

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

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.... ike 0: IKEv1 exchange=Aggressive
id=baf47d0988e9237f/2f405ef3952f6fda len=430 ike 0: in

BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C00000
0010000000100000300101000 ike 0:RemoteSite:4: initiator: aggressive mode get 1st response... ike 0:RemoteSite:4:
VID RFC 3947 4A131c81070358455C5728F20E95452F ike 0:RemoteSite:4: VID DPD
AFCAD71368A1F1C96B8696FC77570100 ike 0:RemoteSite:4: VID FORTIGATE
8299031757A36082C6A621DE000502D7 ike 0:RemoteSite:4: peer is FortiGate/Fortios (v5 b727)

ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3 ike 0:RemoteSite:4: VID
FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000

ike 0:RemoteSite:4: received peer identifier FQDN `remore\\'

ike 0:RemoteSite:4: negotiation result

ike 0:RemoteSite:4: proposal id = 1:

ike 0:RemoteSite:4: protocol id = ISAKMP:

ike 0:RemoteSite:4: trans_id = KEY_IKE.

ike 0:RemoteSite:4: encapsulation = IKE/none

ike 0:RemoteSite:4: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key ?en=128

ike 0:RemoteSite:4: type=OAKLEY_HASH_ALG, val=SHA.

ike 0:RemoteSite:4: type-AUTH_METHOD, val=PRESHARED_KEY.

ike 0:RemoteSite:4: type=OAKLEY_GROUP, val=MODP1024.

ike 0:RemoteSite:4: ISAKMP SA lifetime=86400

ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:

B25B6C9384D8BDB24E3DA3DC90CF5E73

ike 0:RemoteSite:4: PSK authentication succeeded

ike 0:RemoteSite:4: authentication OK

ike 0:RemoteSite:4: add INITIAL-CONTACT

ike 0:RemoteSite:4: enc BAF47D0988E9237F405EF3952F6FDA081004010000000000000080140000181F2E48BF
D8E9D603F ike 0:RemoteSite:4: out

BAF47D0988E9237F405EF3952F6FDA08100401000000000000008C2E3FC9BA061816A 396F009A12

ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140, id=baf47d0988e9237f/2 ike
0:RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

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

A. The remote gateway IP address is 10.0.0.1.

B. It shows a phase 1 negotiation.

C. The negotiation is using AES128 encryption with CBC hash.

D. The initiator has provided remote as its IPsec peer ID.

Correct Answer: BD

QUESTION 8

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

A. Firewall monitor.

B. Policy monitor.

C. Logs.

D. Crashlogs.

Correct Answer: CD

QUESTION 9

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

A. diagnose sniffer packet any `udp port 500\\'

B. diagnose sniffer packet any `udp port 4500\\'

C. diagnose sniffer packet any `esp\\'

D. diagnose sniffer packet any `udp port 500 or udp port 4500\\'

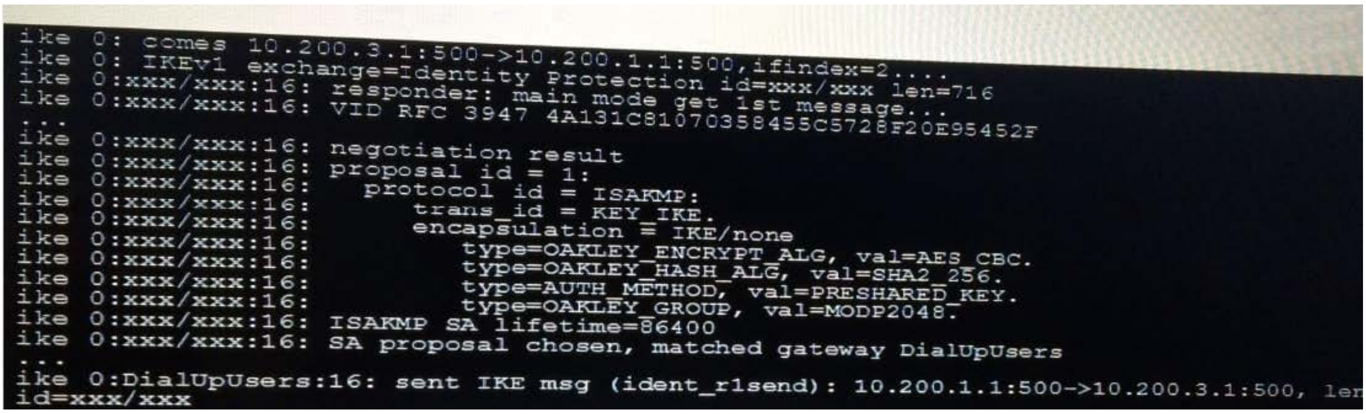
Correct Answer: C

QUESTION 10

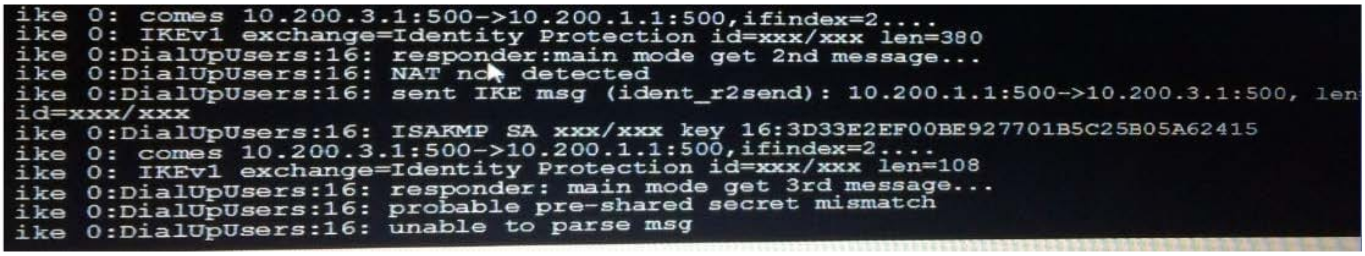
An administrator added the following Ipsec VPN to a FortiGate configuration: configvpn ipsec phasel -interface

edit "RemoteSite" set type dynamic set interface "portl" set mode main set psksecret ENC LCVkCiK2E2PhVUzZe next end config vpn ipsec phase2-interface edit "RemoteSite" set phasel name "RemoteSite" set proposal 3des-sha256 next end However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while

attempting the Ipsec connection. The output is shown in the exhibit.



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



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

What is causing the IPsec problem in the phase 1 ?

A. The incoming IPsec connection is matching the wrong VPN configuration

B. The phrase-1 mode must be changed to aggressive

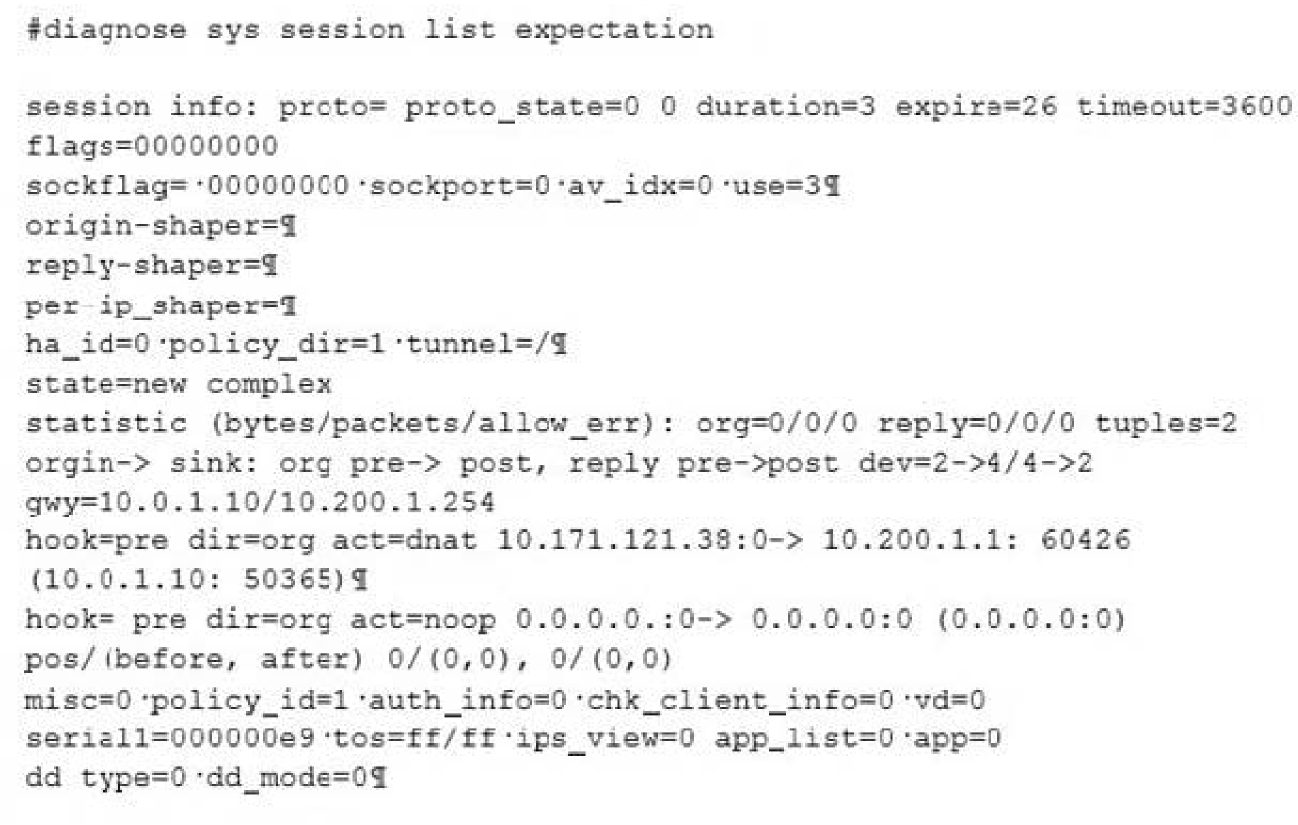
C. The pre-shared key is wrong

D. NAT-T settings do not match

Correct Answer: C

QUESTION 11

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.

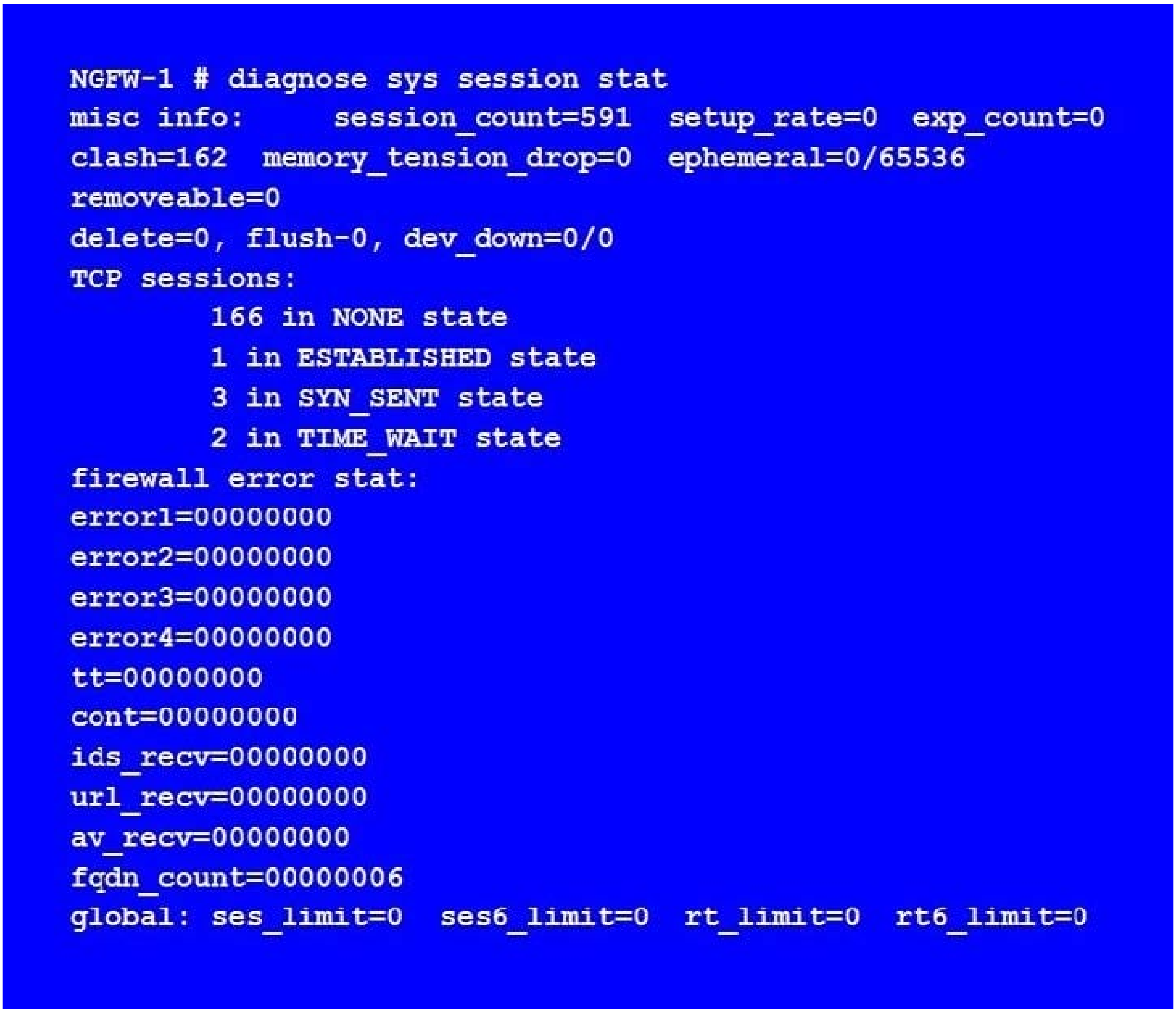
D. It was created by a session helper or ALG.

Correct Answer: A

QUESTION 12

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.

Correct Answer: AD