Fortinet

Exam Questions NSE7

NSE7 Enterprise Firewall - FortiOS 5.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

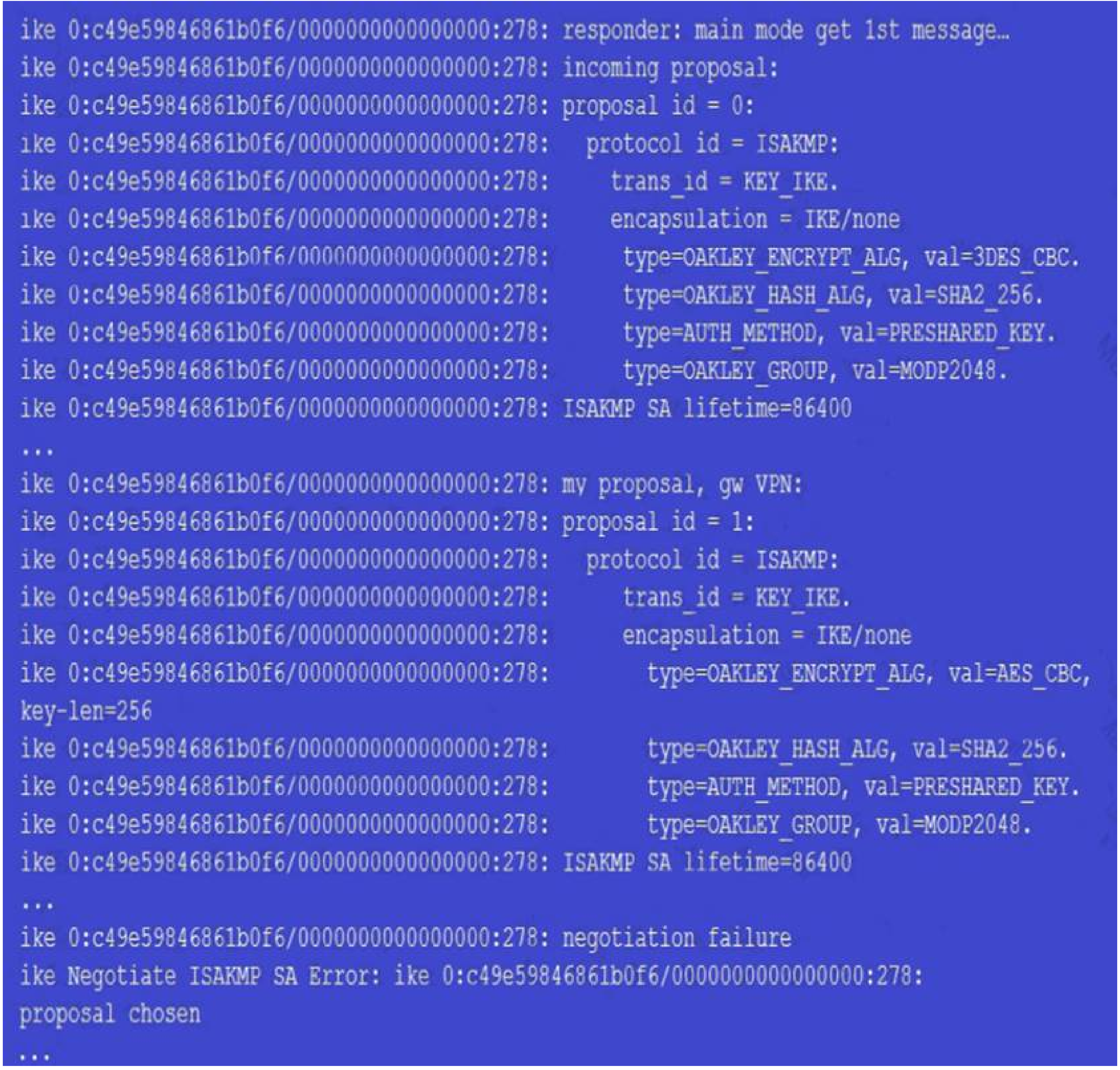
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.



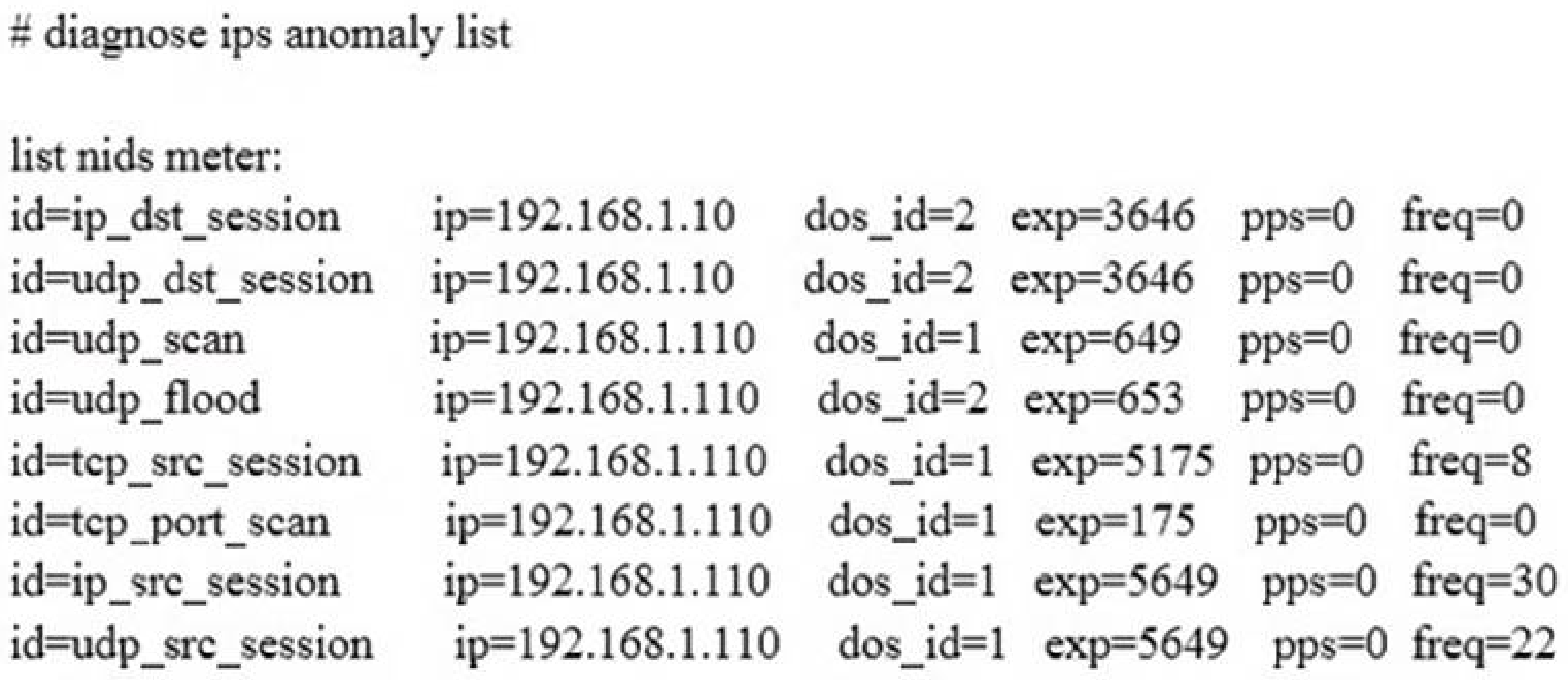
```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     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 2
Examine the output of the ‘diagnose ips anomaly list’ command shown in the exhibit; then answer the question below.



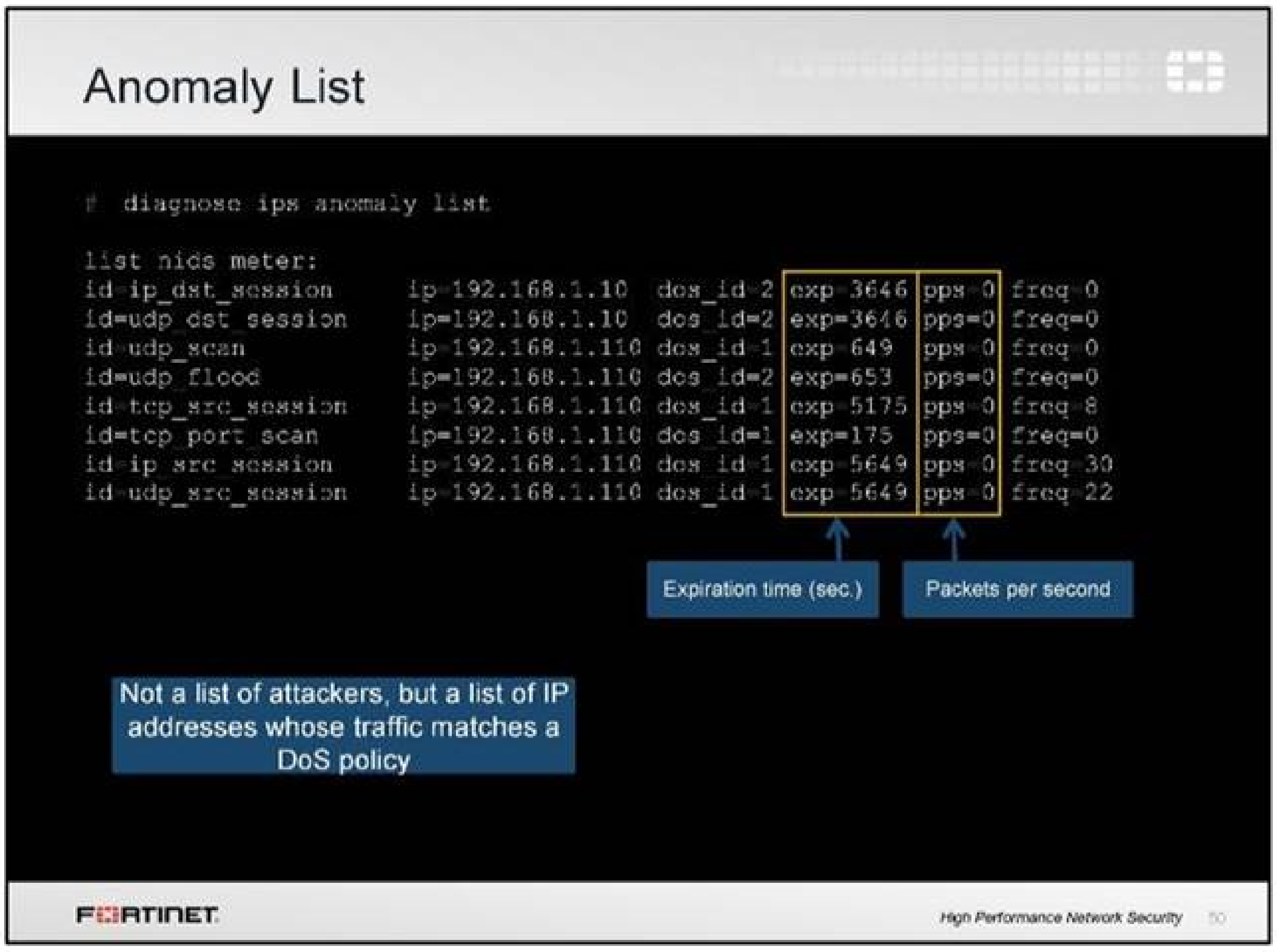
```
# diagnose ips anomaly list

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

Explanation:



Anomaly List

```
# 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
```

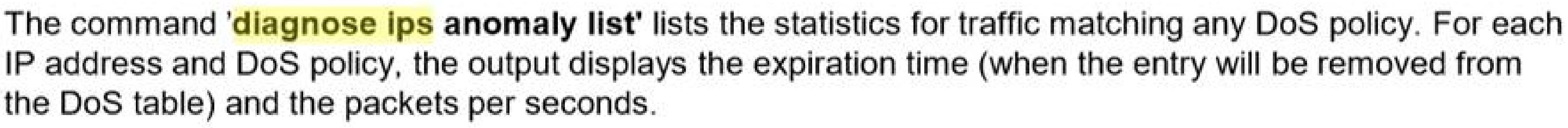
Expiration time (sec.)

Packets per second

Not a list of attackers, but a list of IP addresses whose traffic matches a DoS policy

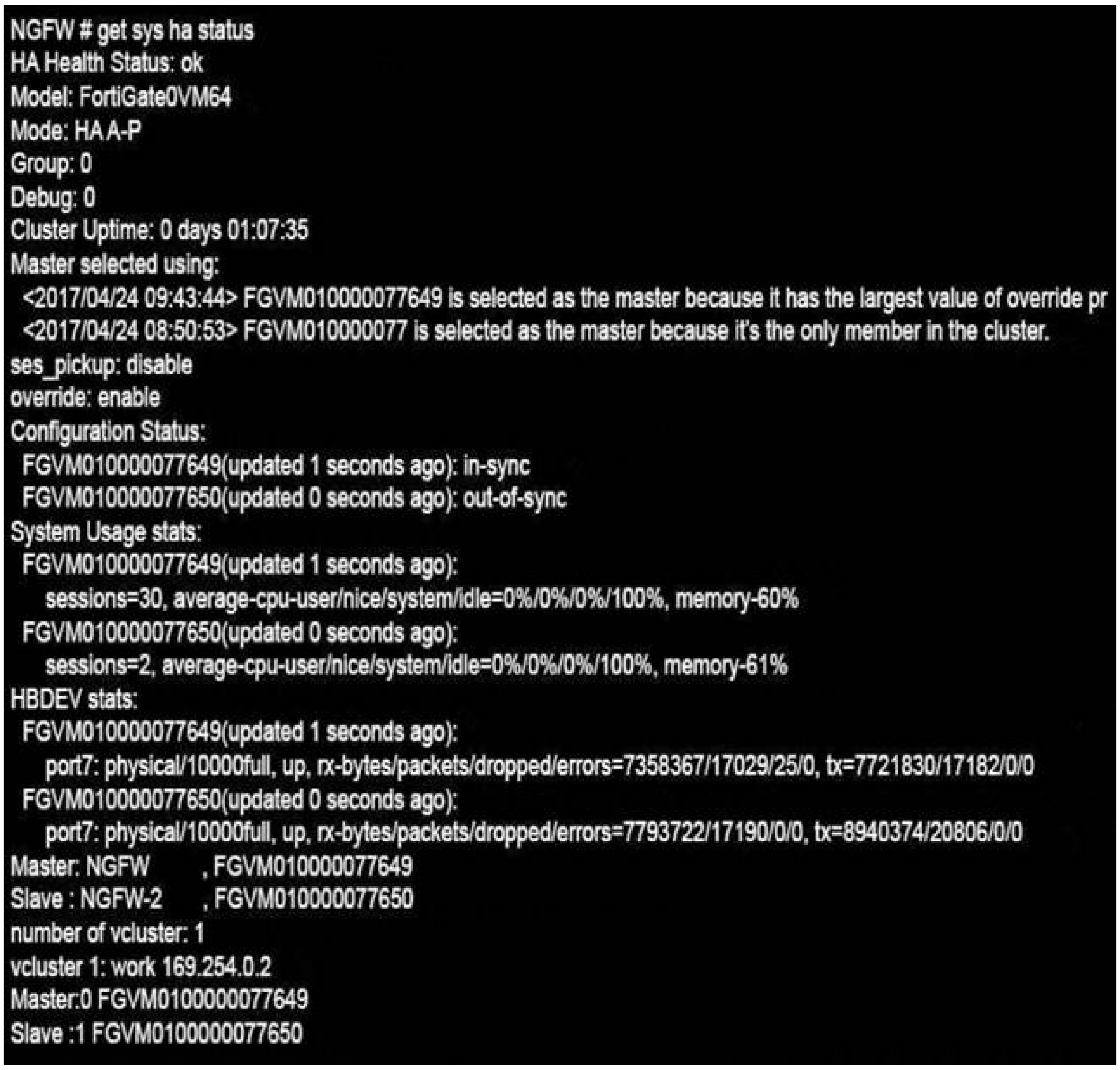
FORTINET

High Performance Network Security



The command '**diagnose ips anomaly list'** lists the statistics for traffic matching any DoS policy. For each IP address and DoS policy, the output displays the expiration time (when the entry will be removed from the DoS table) and the packets per seconds.

NEW QUESTION 3
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
```

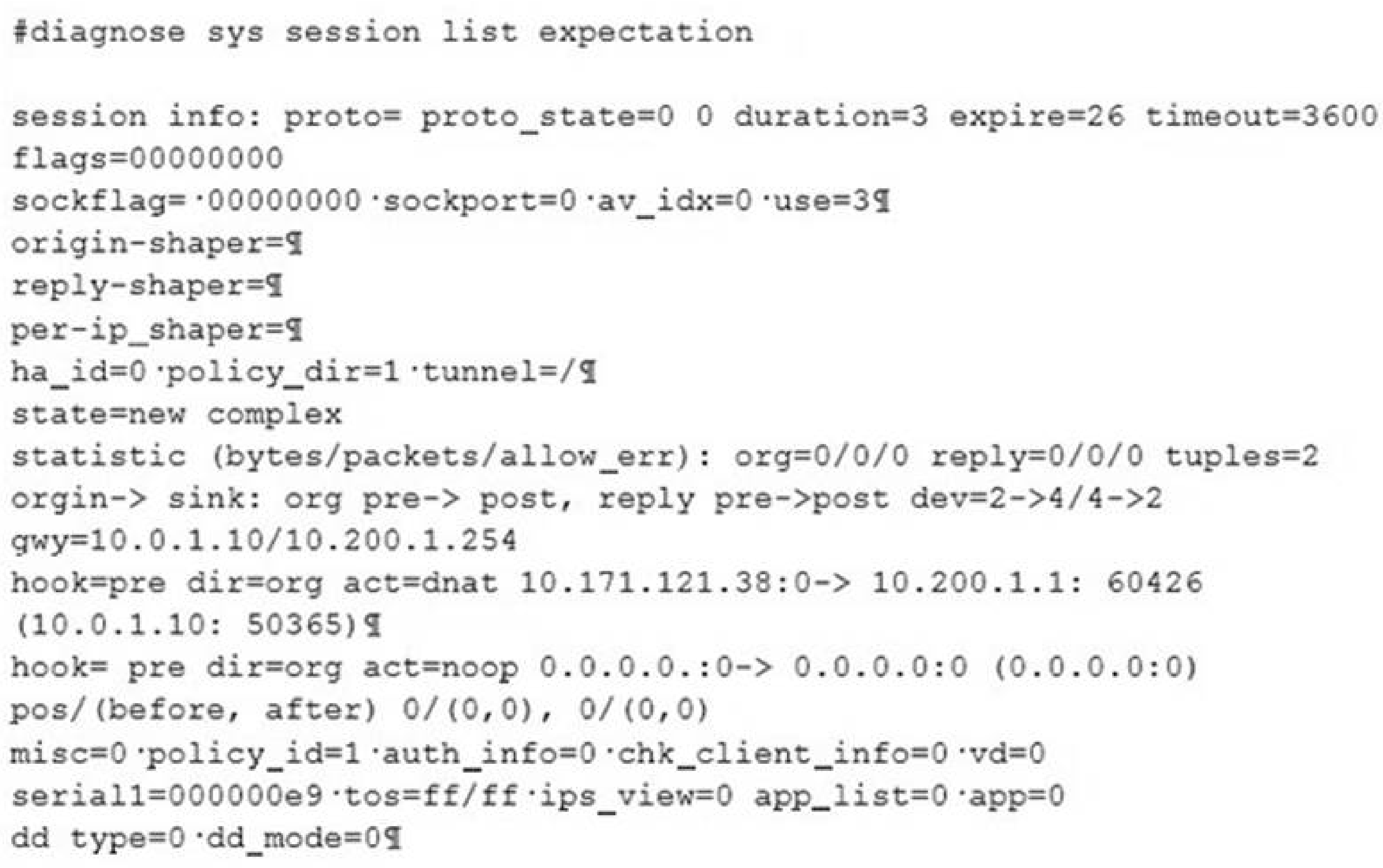
Which statements are correct regarding the output? (Choose two.)

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: AC

NEW QUESTION 4

Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; than answer the question below.



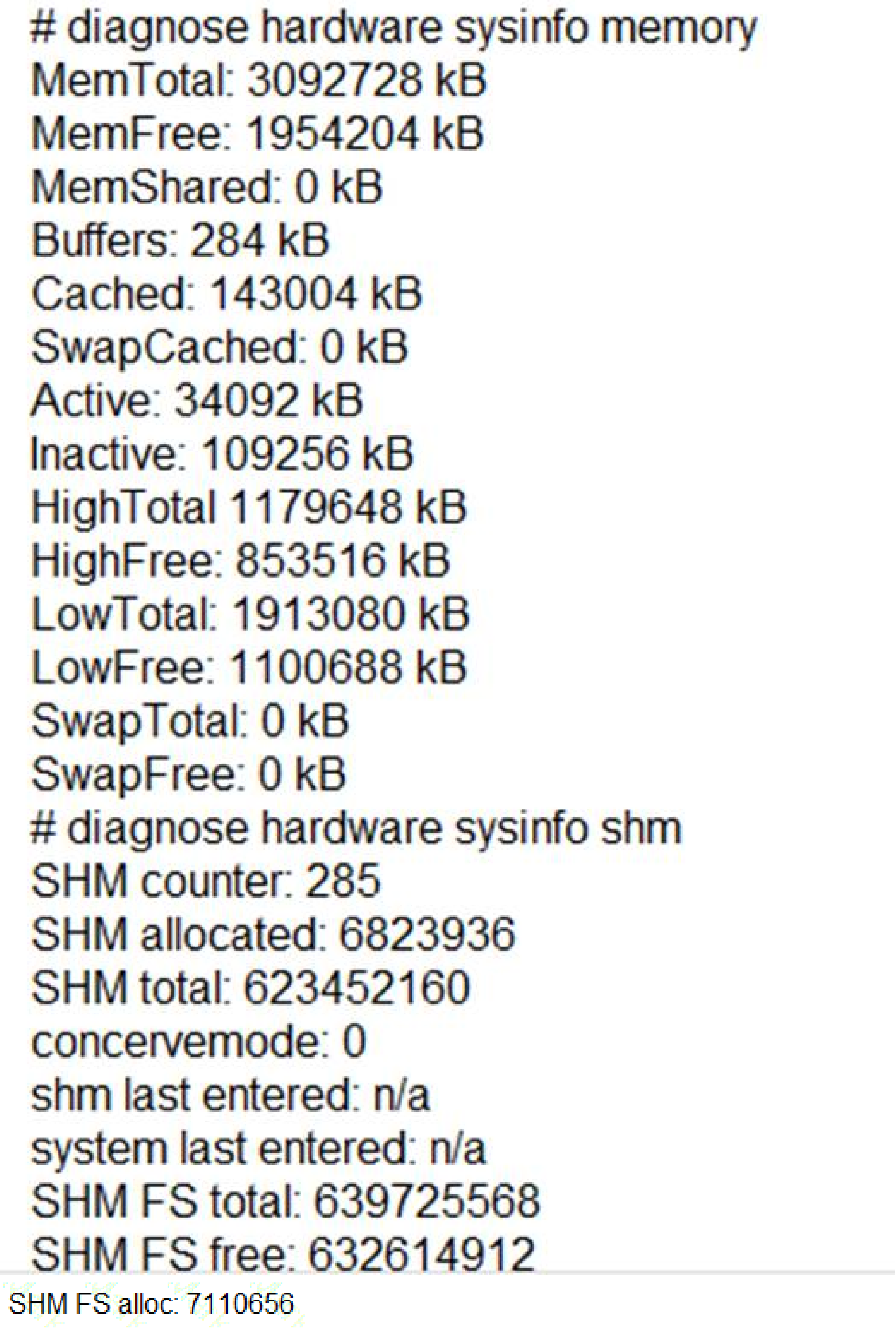
```
#diagnose sys session list expectation

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: A

NEW QUESTION 5
Examine the following partial output from two system debug commands; then answer the question below.



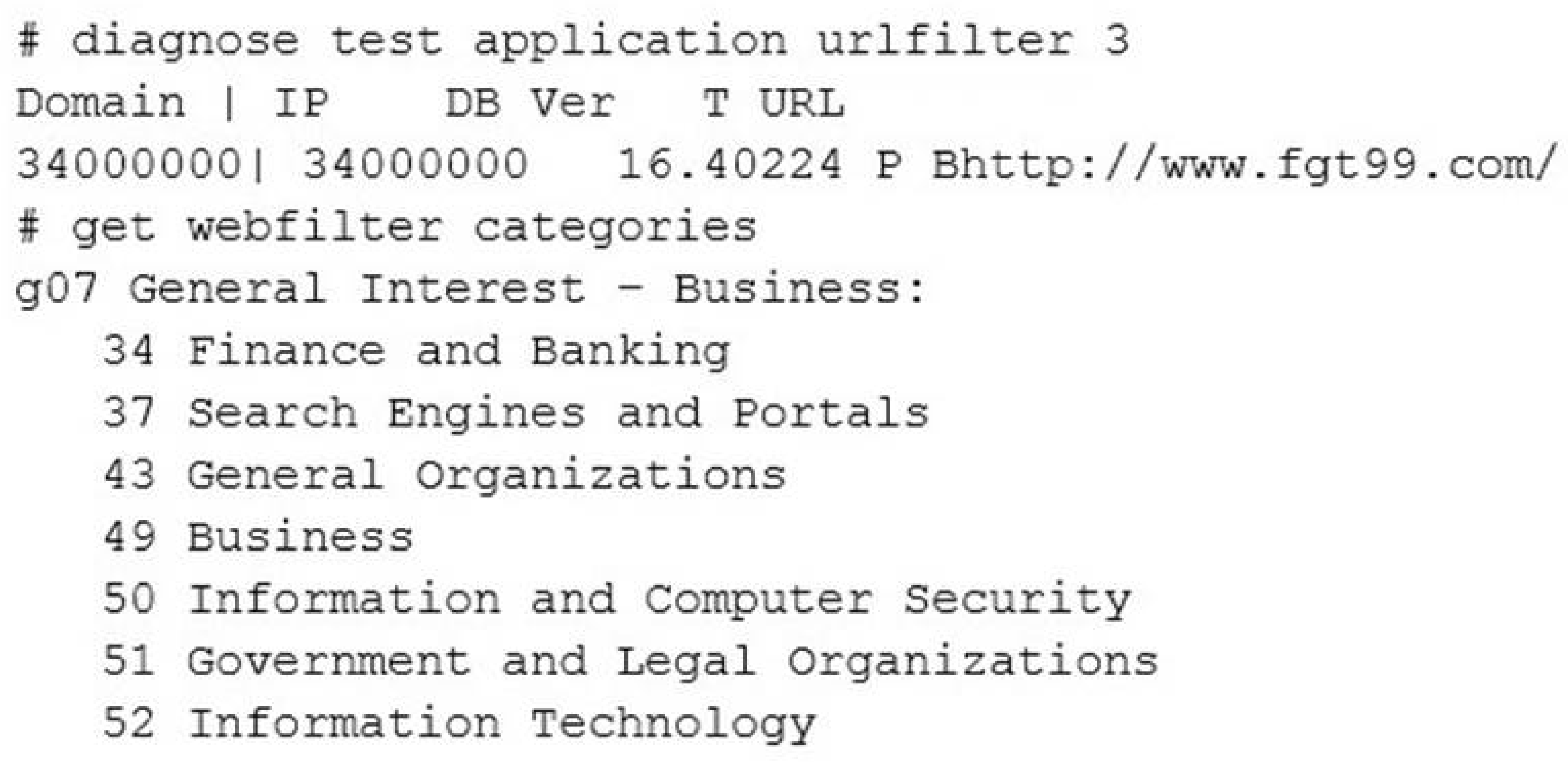
```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose 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 6
Examine the partial output from two web filter debug commands; then answer the question below:



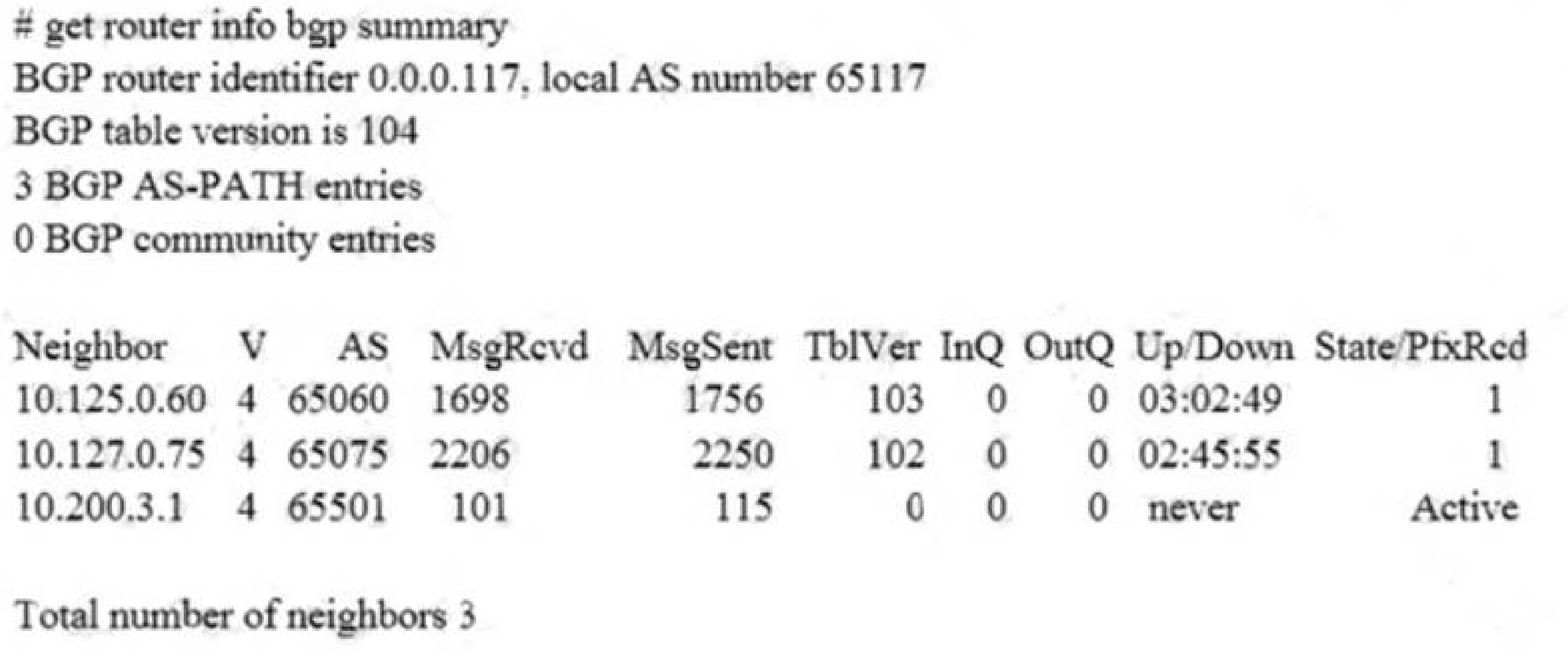
```
# diagnose test application urlfilter 3
Domain | IP     DB Ver    T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General Organizations
   49 Business
   50 Information 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 7
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.

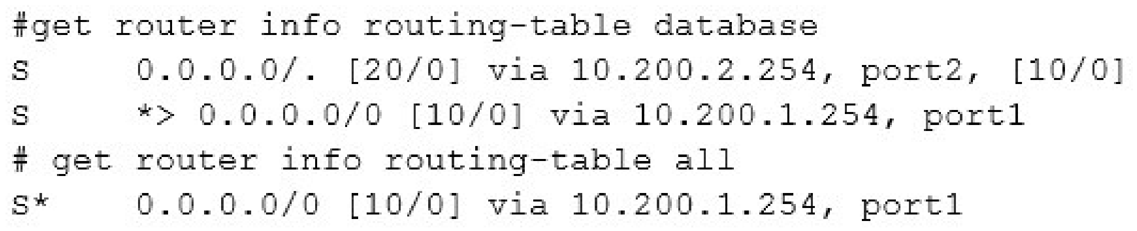
Answer: BC

NEW 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.

Answer: CD

NEW QUESTION 9
Examine the following partial outputs from two routing debug commands; then answer the question below:



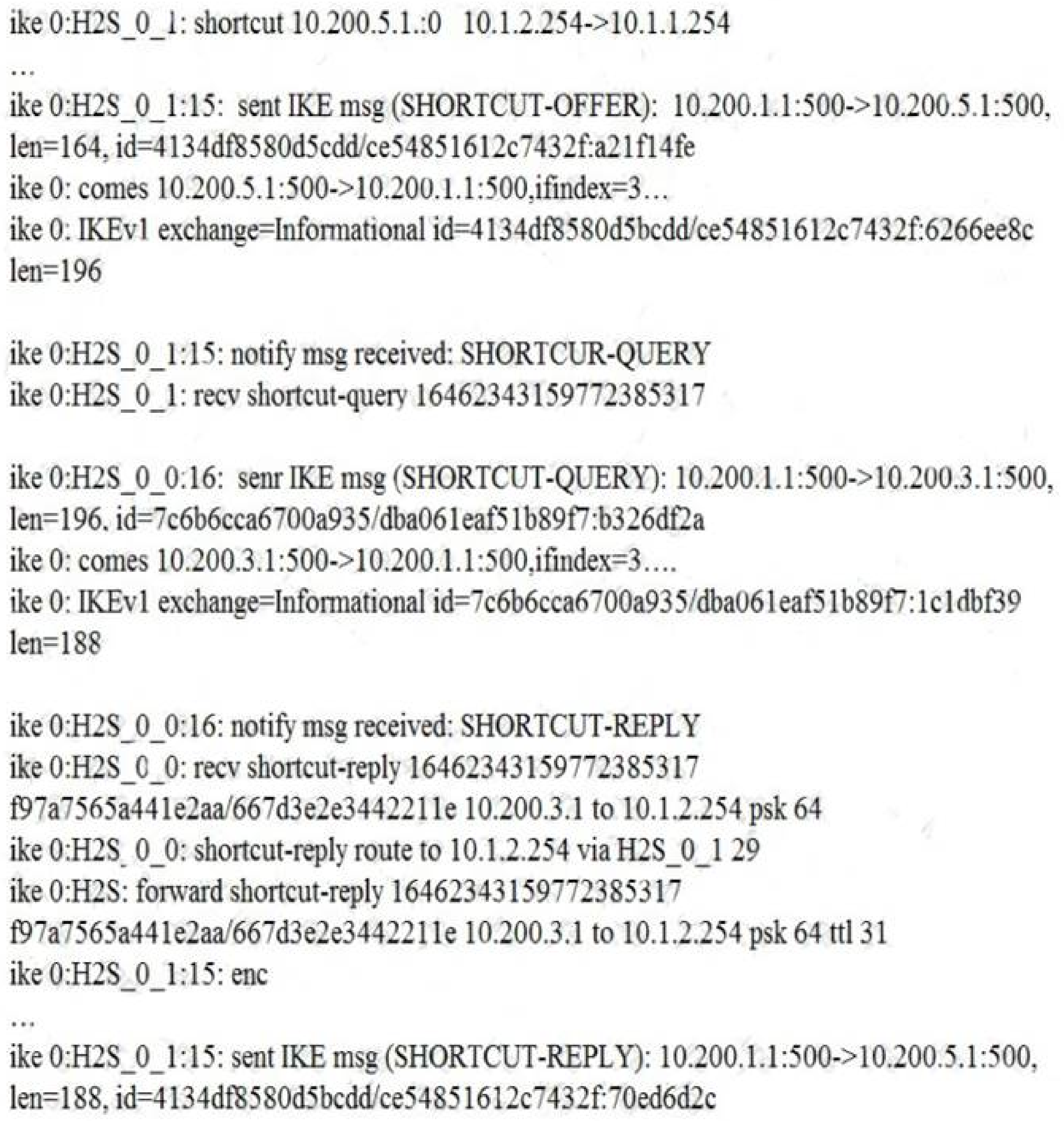
```
#get router info routing-table database
S      0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*     0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

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

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

Answer: A

NEW QUESTION 10
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.



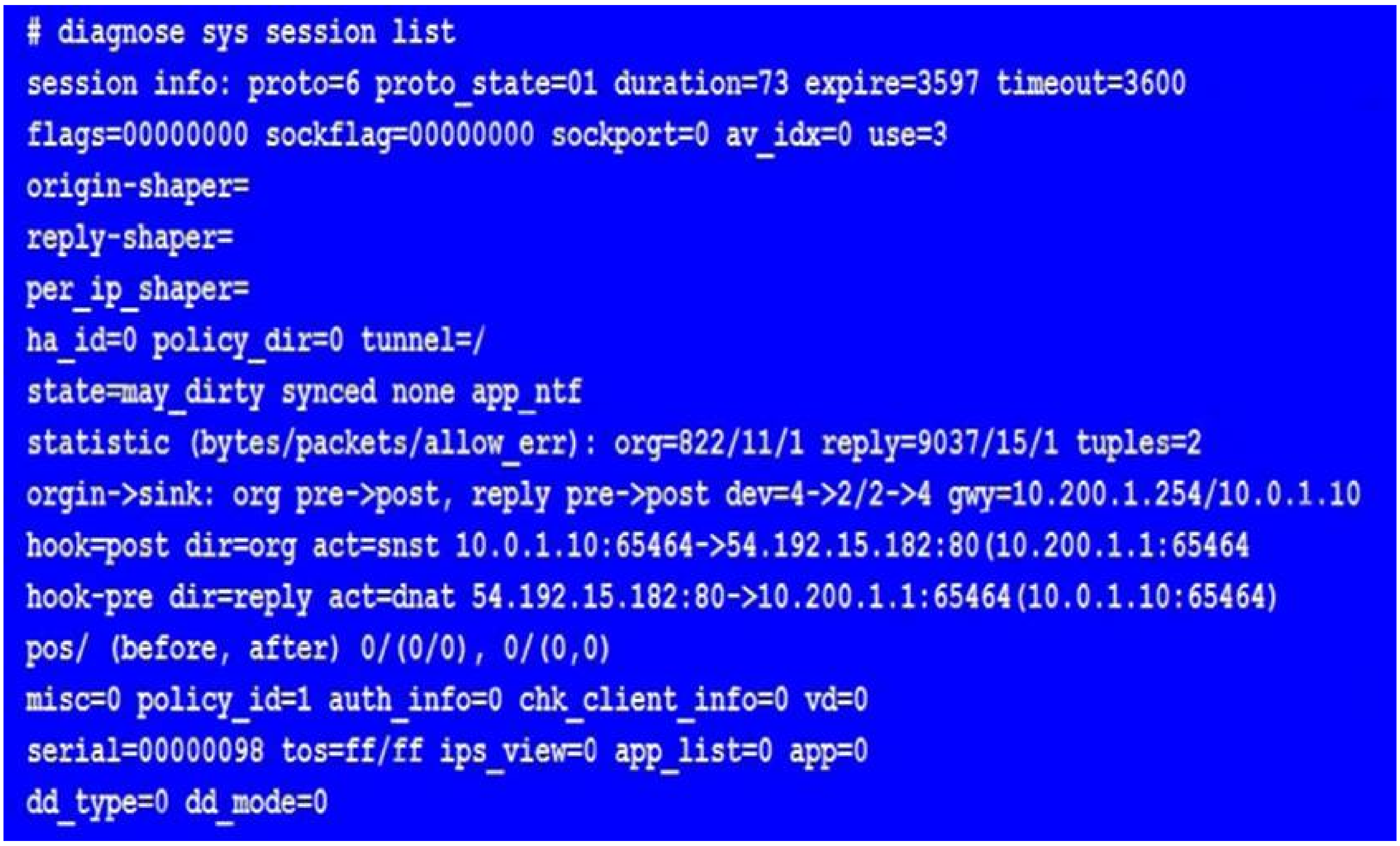
```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254
...
ike 0:H2S_0_1:15:  sent IKE msg (SHORTCUT-OFFER):  10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3…
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16:  senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196. id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
...
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

A. auto-discovery-sender
B. auto-discovery-forwarder
C. auto-discovery-shortcut
D. auto-discovery-receiver

Answer: C

NEW QUESTION 10
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.



```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.182:80(10.200.1.1:65464
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/(0/0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

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

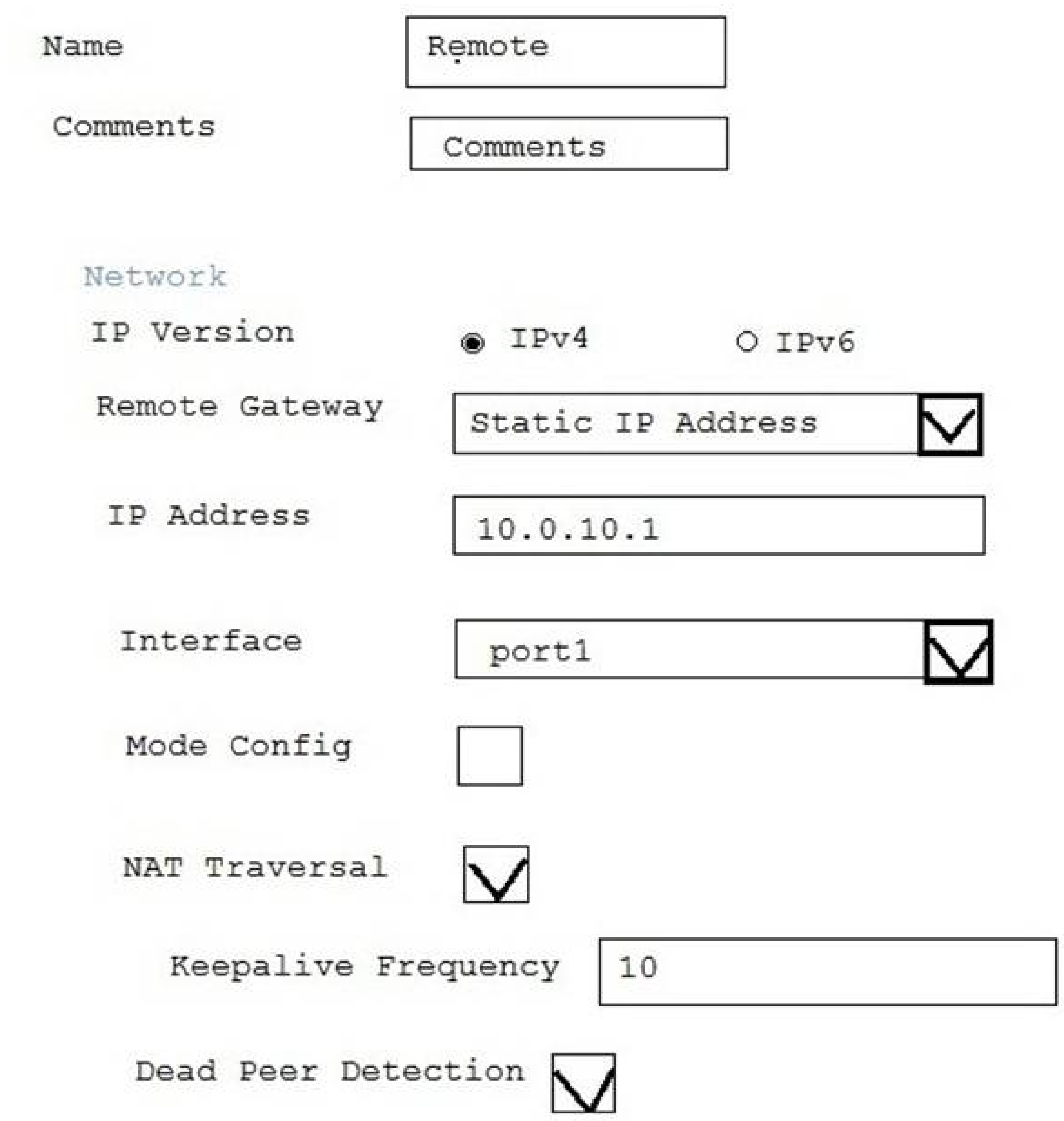
Answer: B

NEW QUESTION 12
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: A

NEW QUESTION 16
Examine the IPsec configuration shown in the exhibit; 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: ☑

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: diagnose vpn ike log-filter src-addr4 10.0.10.1 diagnose debug application ike -1 diagnose debug enable
The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

A. The IKE real time shows the phases 1 and 2 negotiations onl
B. It does not show any more output once the tunnel is up.
C. The log-filter setting is set incorrectl
D. The VPN's traffic does not match this filter.
E. The IKE real time debug shows the phase 1 negotiation onl
F. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
G. The IKE real time debug shows error messages onl
H. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: A

NEW QUESTION 18
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

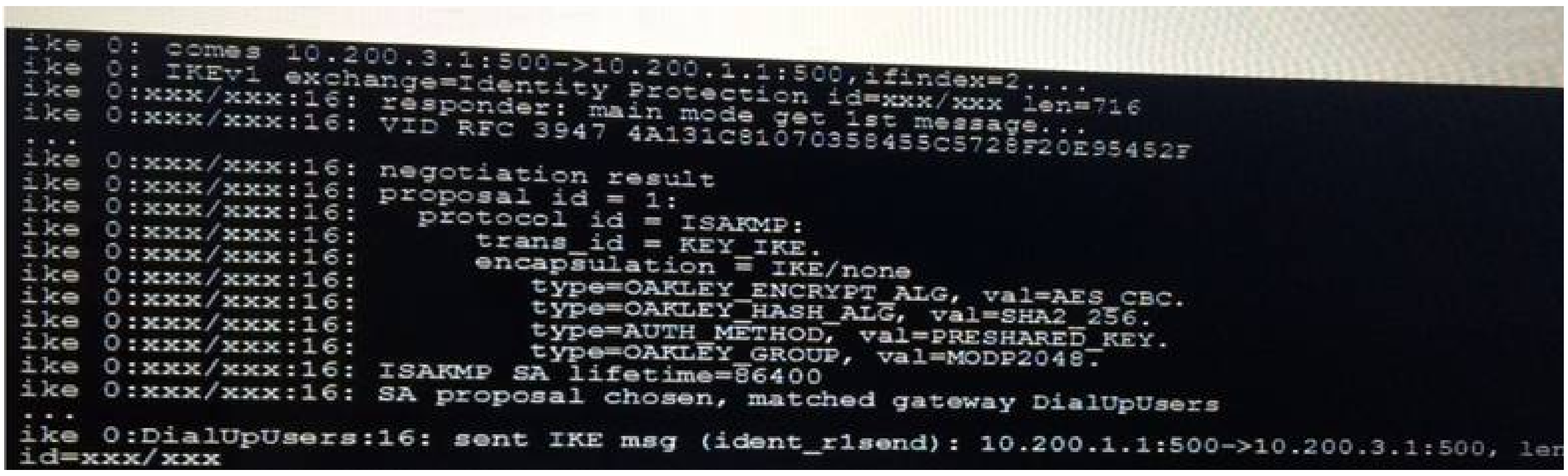
```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7....
ike 0: IKEv1 exchange=Aggressive id=baf47d0988e9237f/2f405ef3952f6fda len=430 ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C0000000100000001000000
ike 0:RemoteSite:4: initiator: aggressive mode get 1st response...
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 –len=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 BAF47D0988E9237F405EF3952F6FDA081004010000000000000080140000181F2E48BFD8E9D603F
ike 0:RemoteSite:4: out BAF47D0988E9237F405EF3952F6FDA08100401000000000000008C2E3FC9BA061816A396F009A12
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.)

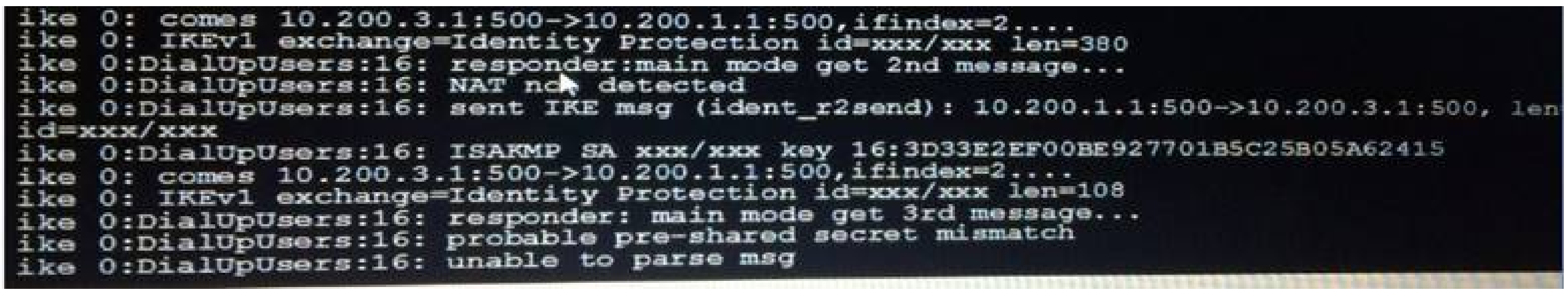
A. The remote gateway IP address is 10.0.0.1.
B. It shows a phase 1 negotiation.
C. The negotiation is using AES128 encryption with CBC hash.
D. The initiator has provided remote as its IPsec peer ID.

Answer: BD

NEW QUESTION 20
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "portl"
set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.



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



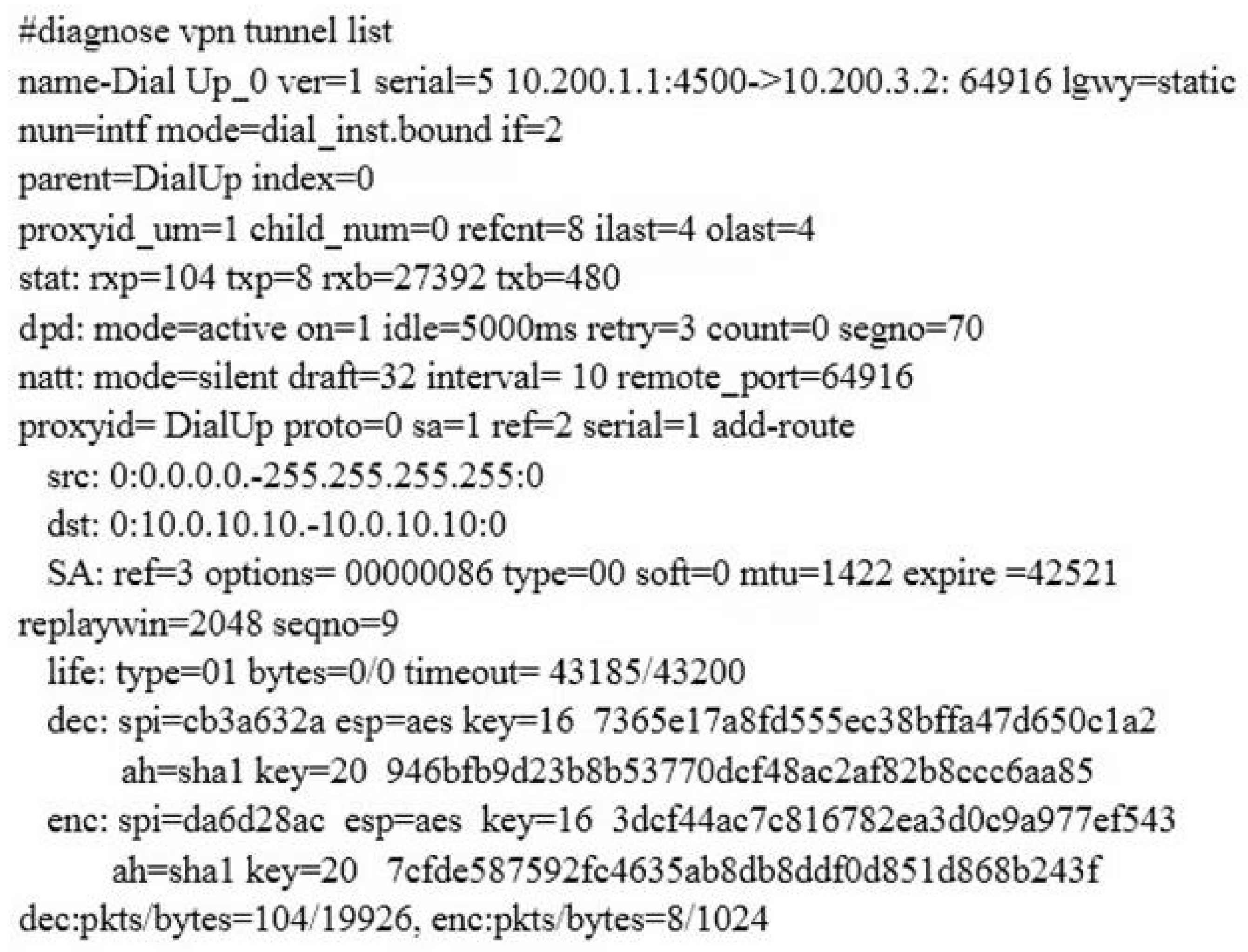
```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=380
ike 0:DialUpUsers:16: responder:main mode get 2nd message...
ike 0:DialUpUsers:16: NAT not detected
ike 0:DialUpUsers:16: sent IKE msg (ident_r2send): 10.200.1.1:500->10.200.3.1:500,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

What is causing the IPsec problem in the phase 1 ?

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

Answer: C

NEW QUESTION 21
Examine the output from the ‘diagnose vpn tunnel list’ command shown in the exhibit; then answer the question below.



```
#diagnose vpn tunnel list
name-Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2: 64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refcnt=8 ilast=4 olast=4
stat: rxp=104 txp=8 rxb=27392 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt: mode=silent draft=32 interval= 10 remote_port=64916
proxyid= DialUp proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0.-255.255.255.255:0
  dst: 0:10.0.10.10.-10.0.10.10:0
  SA: ref=3 options= 00000086 type=00 soft=0 mtu=1422 expire =42521
replaywin=2048 seqno=9
  life: type=01 bytes=0/0 timeout= 43185/43200
  dec: spi=cb3a632a esp=aes key=16  7365e17a8fd555ec38bffa47d650c1a2
       ah=sha1 key=20  946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
  enc: spi=da6d28ac  esp=aes  key=16  3dcf44ac7c816782ea3d0c9a977ef543
       ah=sha1 key=20  7cfde587592fc4635ab8db8ddf0d851d868b243f
dec:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

Which command can be used to sniffer the ESP traffic for the VPN DialUP_0?

A. diagnose sniffer packet any ‘port 500’
B. diagnose sniffer packet any ‘esp’
C. diagnose sniffer packet any ‘host 10.0.10.10’
D. diagnose sniffer packet any ‘port 4500’

Answer: B

NEW QUESTION 24
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.

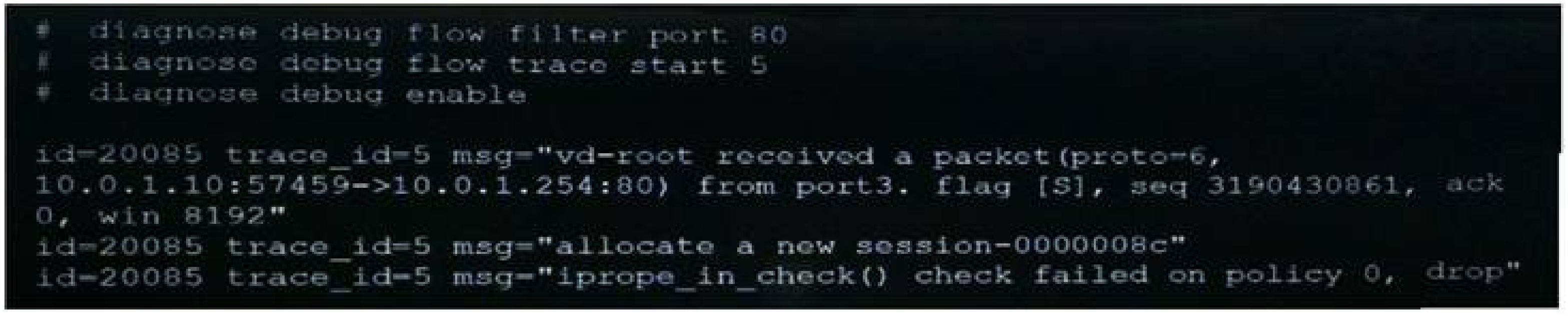
Answer: BC

NEW QUESTION 29
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

NEW QUESTION 30
An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:



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

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

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

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

Answer: AC

NEW QUESTION 34
Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

A. 1
B. 2
C. 3
D. 4

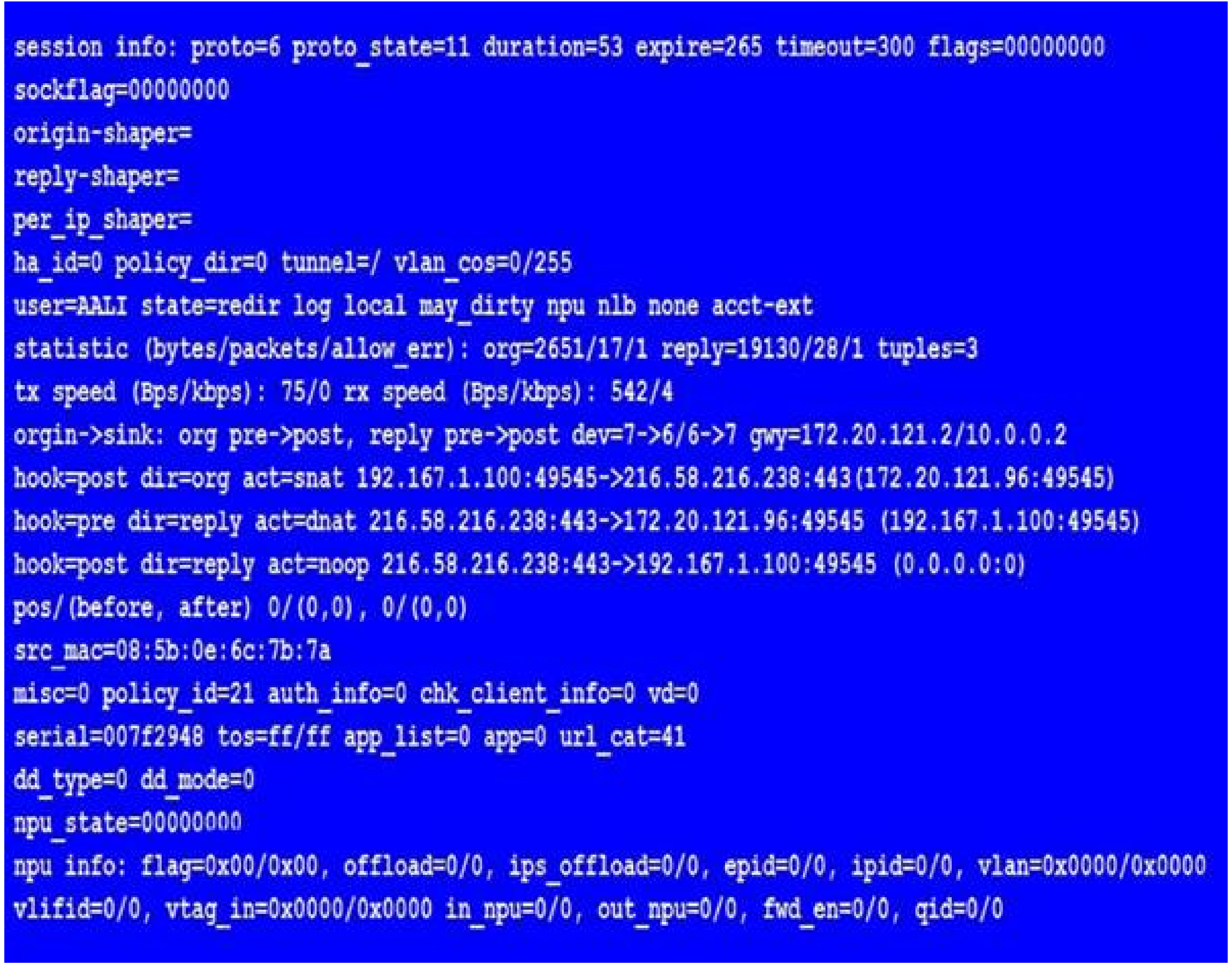
Answer: B

NEW QUESTION 39
What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

A. A process crash.
B. Configuration changes.
C. Changes in the status of any of the FortiGuard licenses.
D. System entering to and leaving from the proxy conserve mode.

Answer: AD

NEW QUESTION 41
View the exhibit, which contains an entry in the session table, and then answer the question below.



```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
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)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
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
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 one of the following statements is true regarding FortiGate’s inspection of this session?

A. FortiGate applied proxy-based inspection.
B. FortiGate forwarded this session without any inspection.
C. FortiGate applied flow-based inspection.
D. FortiGate applied explicit proxy-based inspection.

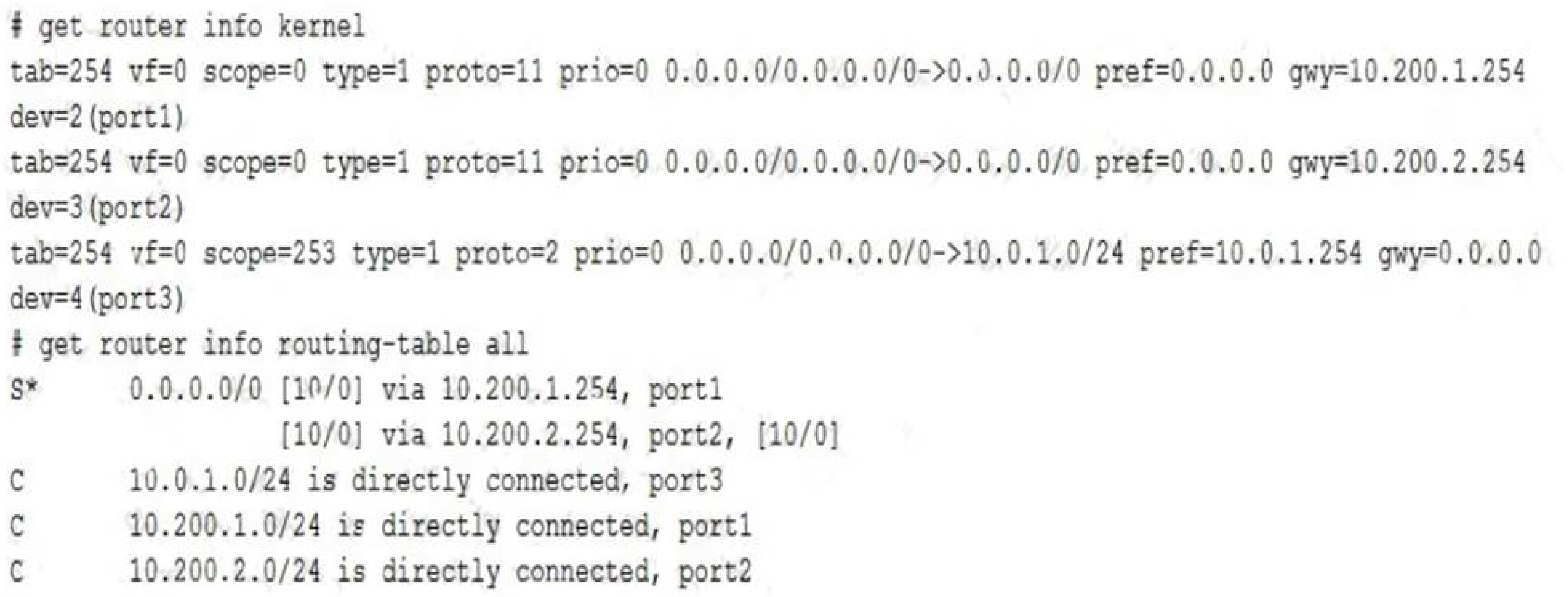
Answer: B

NEW QUESTION 43
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI)?

A. FortiGate uses the Issued To: field in the server’s certificate.
B. FortiGate switches to the full SSL inspection method to decrypt the data.
C. FortiGate blocks the request without any further inspection.
D. FortiGate uses the requested URL from the user’s web browser.

Answer: D

NEW QUESTION 48
View these partial outputs from two routing debug commands:



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

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

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

Answer: C

NEW QUESTION 49
......

Relate Links

100% Pass Your NSE7 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/