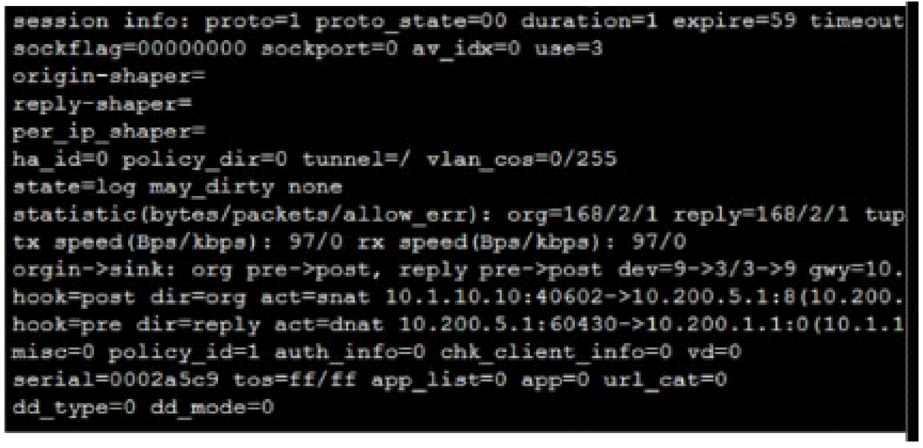
# Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

**https://www.2passeasy.com/dumps/NSE7_EFW-7.0/**

**NEW QUESTION 1**
Refer to the exhibit, which shows a session entry. Which statement about this session is true?



```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
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 tup
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.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
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
```

A. It is an ICMP session from 10.1.10.10 to 10.200.5. 1.
B. It is a TCP session in close_wait state, from 10.
C. 10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

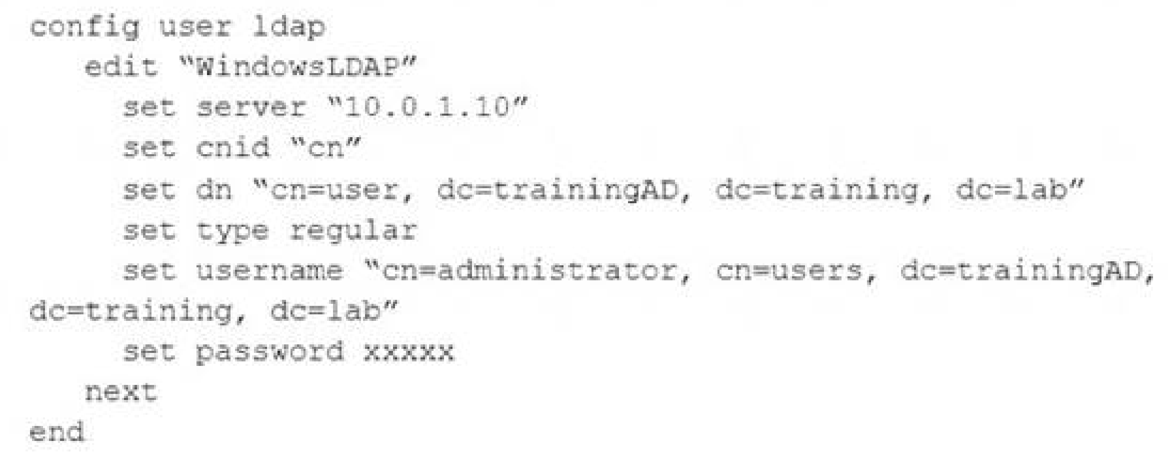
**Answer:** A

**NEW QUESTION 2**
When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

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

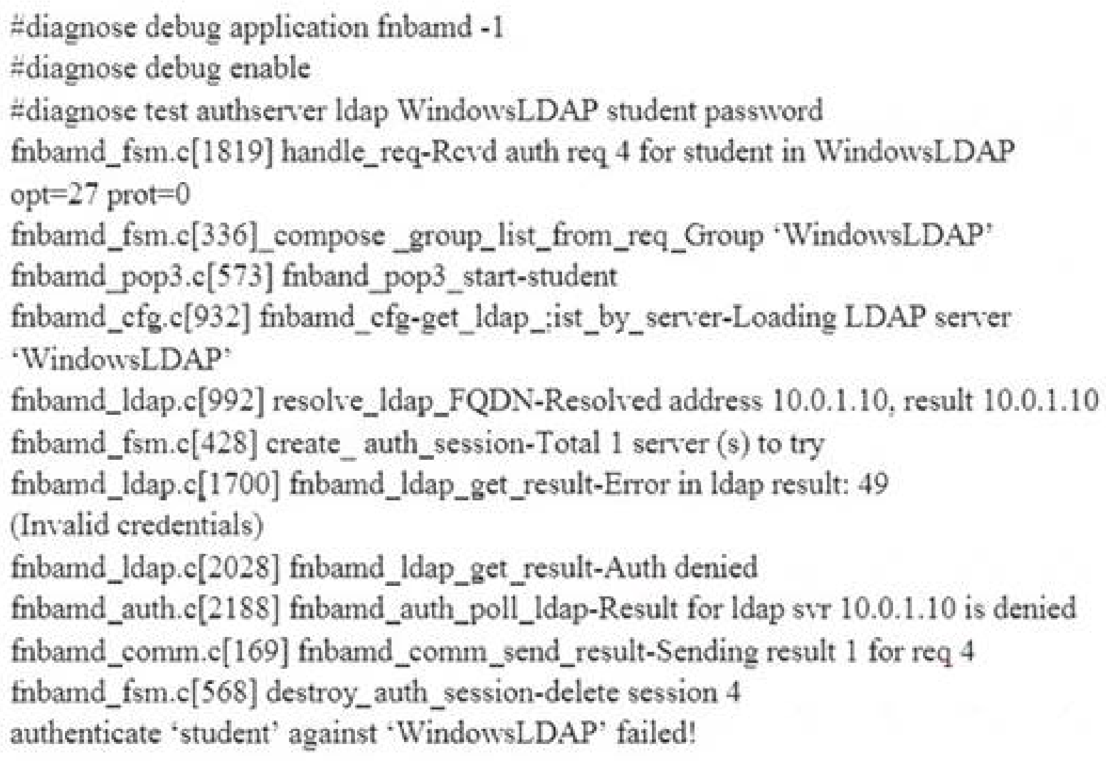
**Answer:** B

**NEW QUESTION 3**
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=user, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
     set password xxxxx
   next
end
```

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:



```
#diagnose debug application fnbamd -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 4 for student in WindowsLDAP
opt=27 prot=0
fnbamd_fsm.c[336]_compose _group_list_from_req_Group ‘WindowsLDAP’
fnbamd_pop3.c[573] fnband_pop3_start-student
fnbamd_cfg.c[932] fnbamd_cfg-get_ldap_;ist_by_server-Loading LDAP server
‘WindowsLDAP’
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_ auth_session-Total 1 server (s) to try
fnbamd_ldap.c[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate ‘student’ against ‘WindowsLDAP’ failed!
```

Based on the above output, what FortiGate LDAP settings must the administer check? (Choose two.)

A. cnid.
B. username.

C. password.
D. dn.

**Answer:** BC

**Explanation:**
https://kb.fortinet.com/kb/viewContent.do?externalId=13141

**NEW QUESTION 4**
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

**Explanation:**
diagnose debug crashlog read
275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05
13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated278: 2014-08-06 11:05:47 service=kernel conserve=on free=”45034 pages” red=”45874 pages” msg=”Kernel279: 2014-08-06 11:05:47 enters conserve mode”280: 2014-08-06 13:07:16 service=kernel conserve=exit free=”86704 pages” green=”68811 pages”281: 2014-08-06 13:07:16 msg=”Kernel leaves conserve mode”282: 2014-08-06
13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

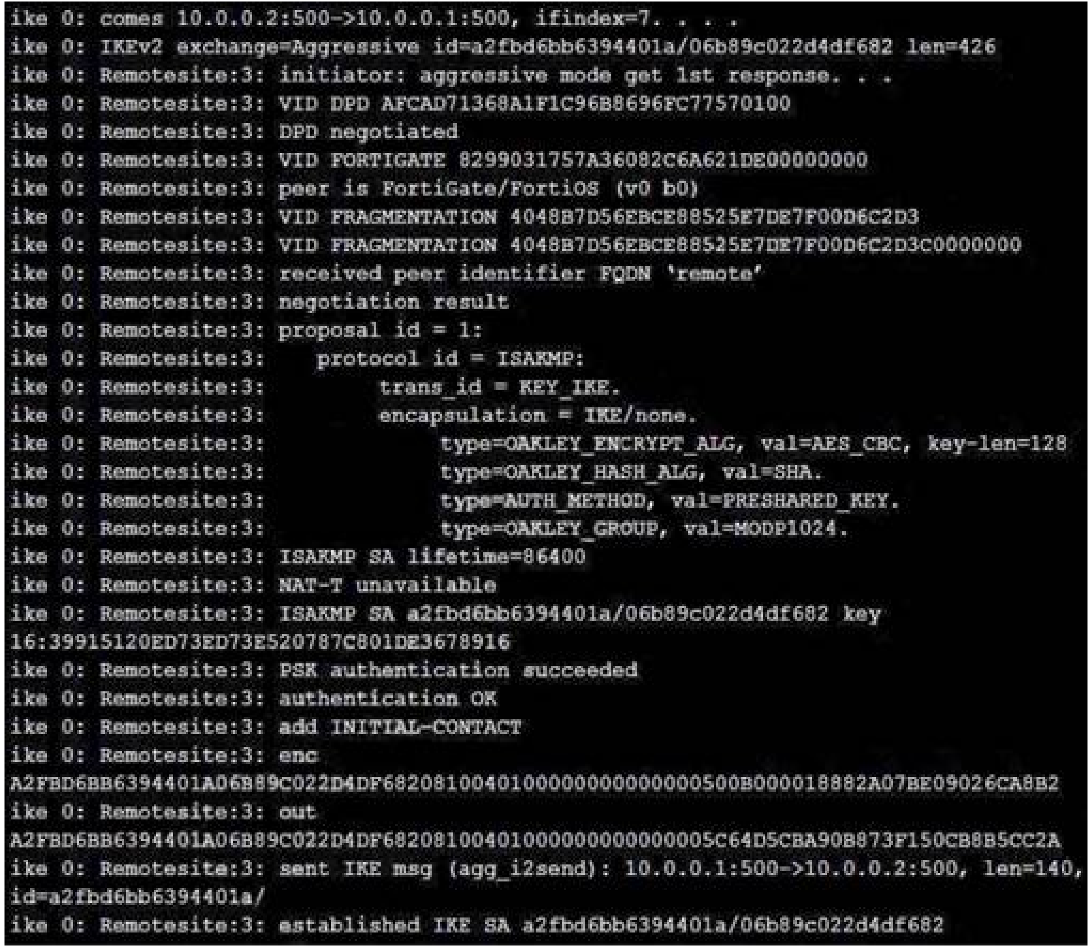
**NEW QUESTION 5**
What is the purpose of an internal segmentation firewall (ISFW)?

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 6**
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: IKEv2 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
16:39915120ED73ED73E520787C801DE3678916
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
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07BE09026CA8B2
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 remote gateway IP address is 10.0.0.1.
B. The initiator provided remote as its IPsec peer ID.
C. It shows a phase 1 negotiation.
D. The negotiation is using AES128 encryption with CBC hash.

**Answer:** BC

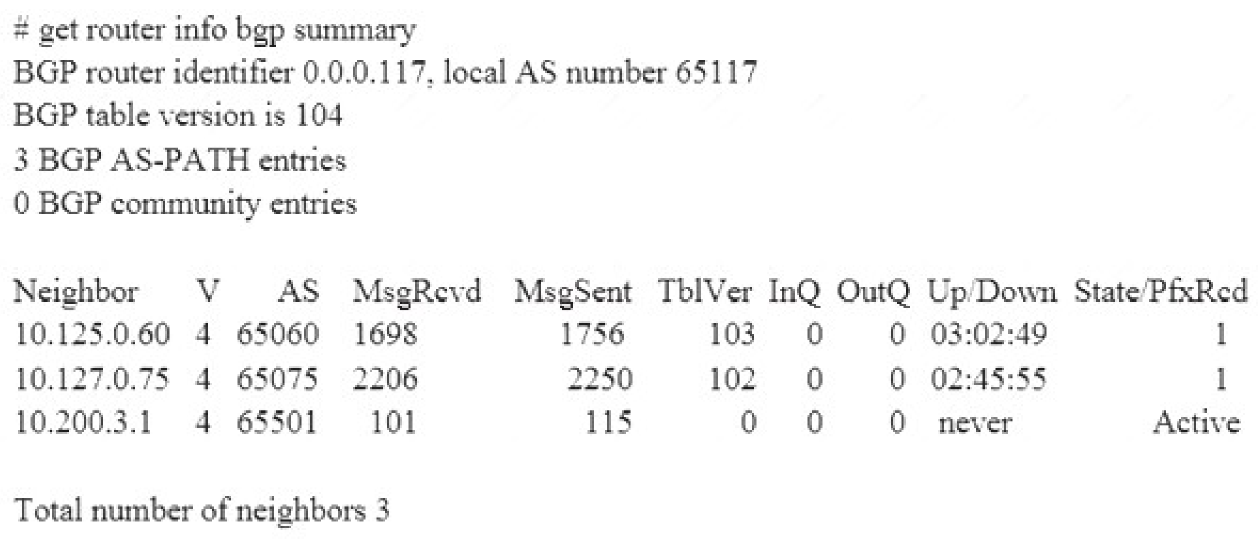
**NEW QUESTION 7**
An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

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’

**Answer:** C

**Explanation:**
Capture IKE Traffic without NAT:diagnose sniffer packet ‘host and udp port 500’
————————————————————————————————————————-Capture ESP Traffic without NAT:diagnose sniffer packet any ‘host and esp’
————————————————————————————————————————-Capture IKE and ESP with NAT-T:diagnose sniffer packet any ‘host and (udp port 500 or udp port 4500)’

**NEW QUESTION 8**
View the exhibit, which contains the output of a BGP debug command, and then answer the question below.



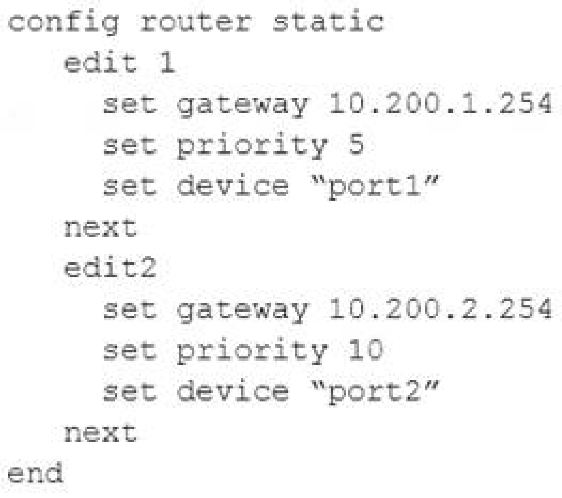
```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

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.

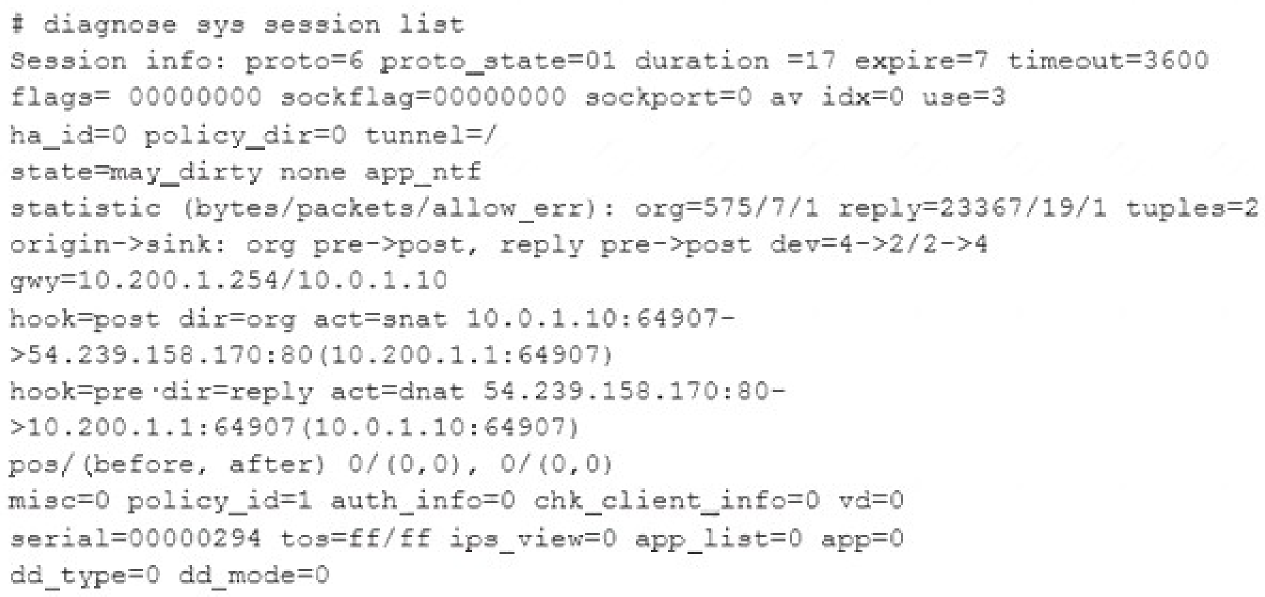
**Answer:** AD

**NEW QUESTION 9**
A FortiGate has two default routes:



```
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
```

All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:



```
# 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. The session would be deleted, and the client would need to start a new session.
B. The session would remain in the session table, and its traffic would start to egress from port2.
C. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
D. The session would remain in the session table, and its traffic would still egress from port1.

**Answer:** D

**NEW QUESTION 10**
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

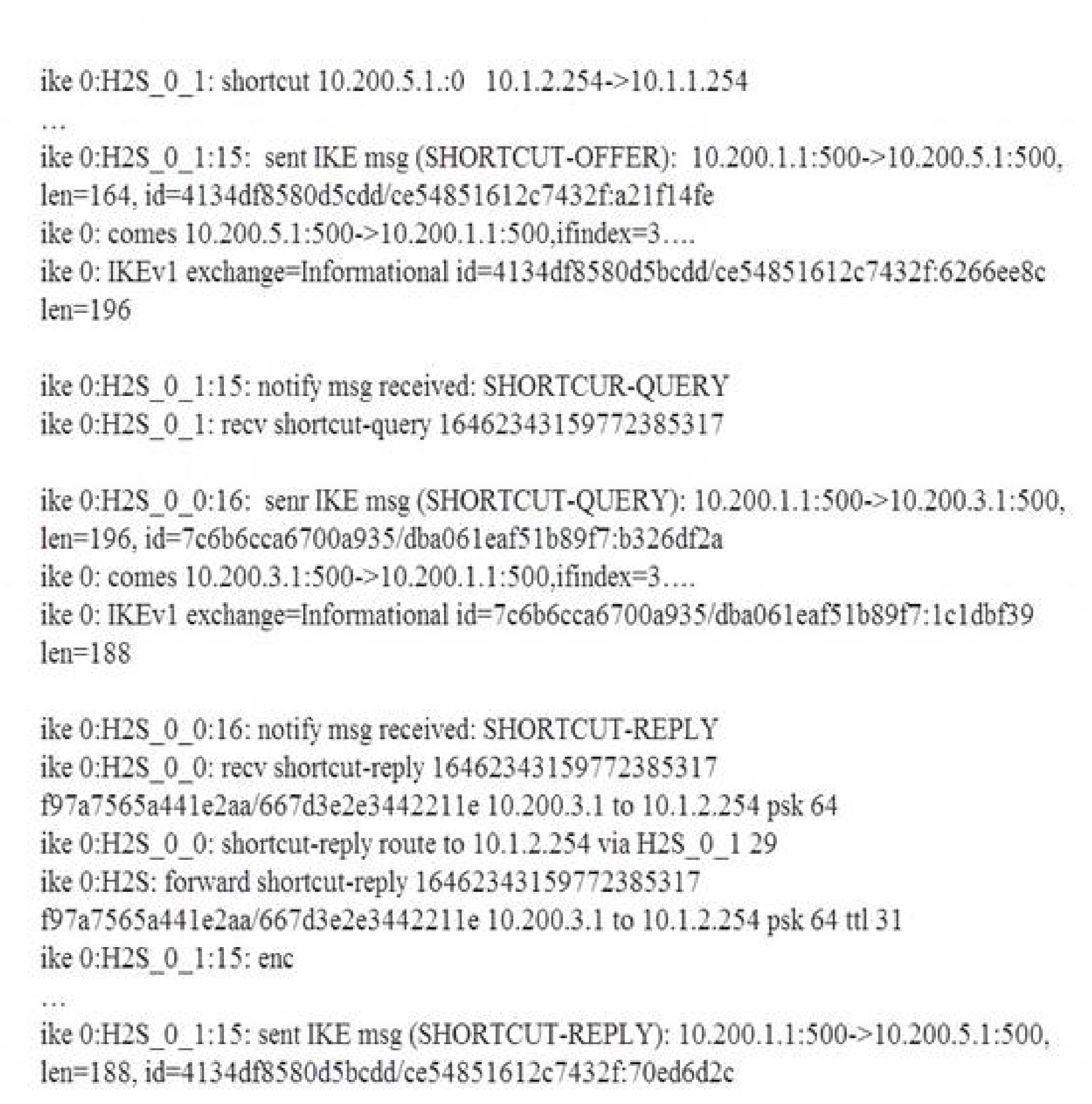
**NEW QUESTION 10**
An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients 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.

**NEW QUESTION 15**
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.



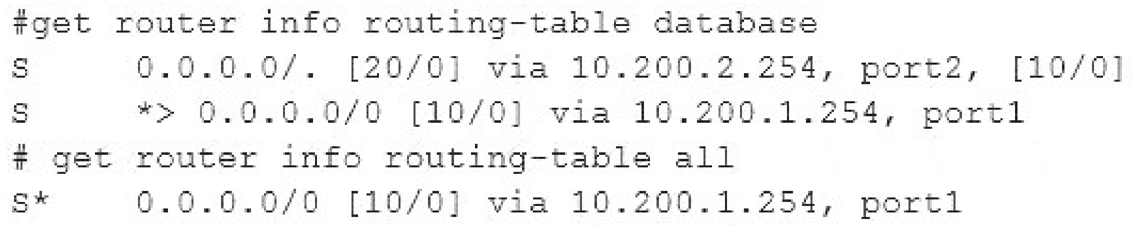
```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254
...
ike 0:H2S_0_1:15:  sent IKE msg (SHORTCUT-OFFER):  10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c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

**NEW QUESTION 18**
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
```

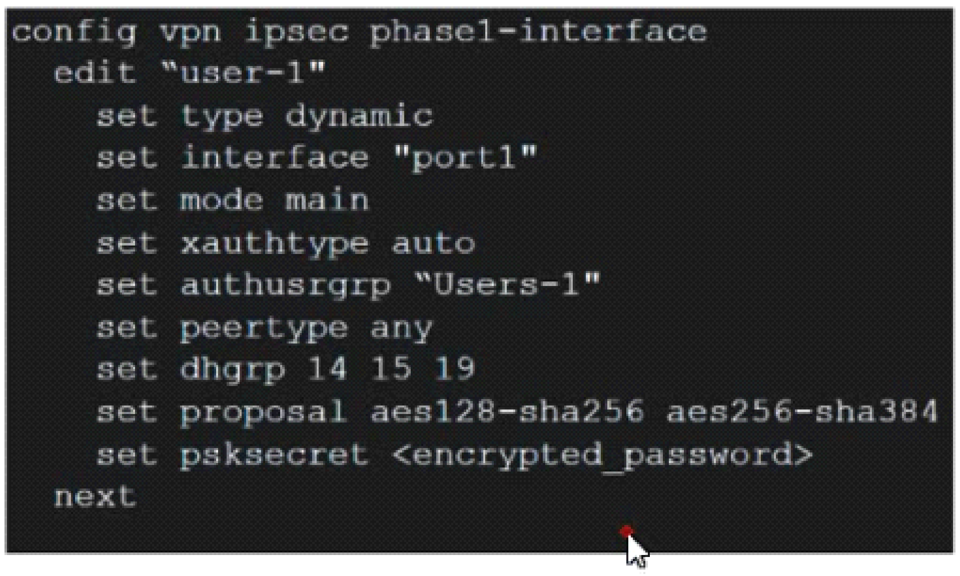
Why the default route using port2 is not displayed in the output of the second command?

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:** C

**Explanation:**
http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103

**NEW QUESTION 23**
Refer to the exhibits.



```
config vpn ipsec phase1-interface
  edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
  next
```

Which contain the partial configurations of two VPNs on FortiGate.
An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.
Which two changes must administrator make to fix the issue? (Choose two.)

A. Use different pre-shared keys on both VPNs
B. Enable Mode Config on both VPNs.
C. Set up specific peer IDs on both VPNs.
D. Change to aggressive mode on both VPNs.

**Answer:** CD

**NEW QUESTION 25**
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 30**
A FortiGate's portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the local flag on.
B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
C. One session has the proxy flag on, the other one does not.
D. One of the sessions has the IP address of port2 as the source IP address.

**Answer:** AD

**NEW QUESTION 32**
An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug:
diagnose debug application ike-1 diagnose debug enable
In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

A. Phase1; IKE mode configuration; XAuth; phase 2.
B. Phase1; XAuth; IKE mode configuration; phase2.
C. Phase1; XAuth; phase 2; IKE mode configuration.
D. Phase1; IKE mode configuration; phase 2; XAuth.

**Answer:** B

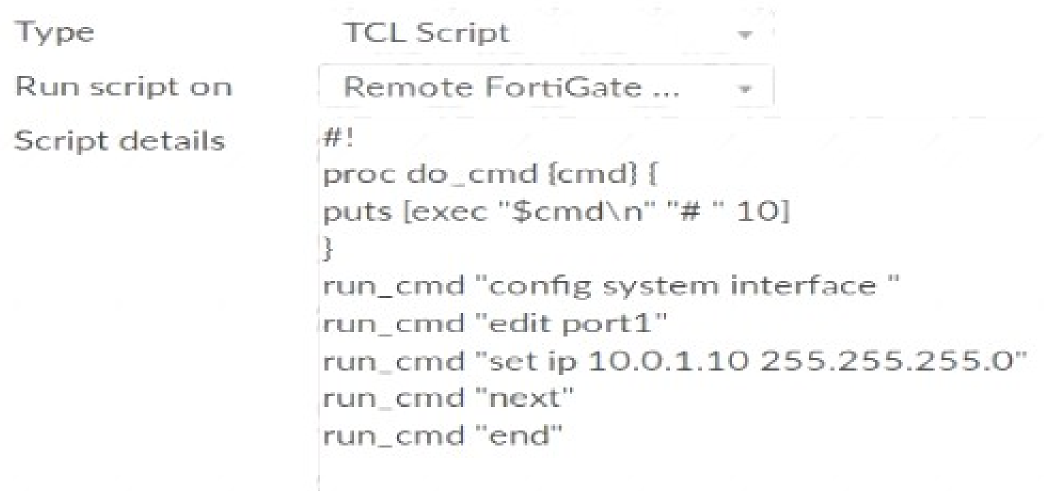
**Explanation:**
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet

**NEW QUESTION 33**
Which statement about NGFW policy-based application filtering is true?

A. After the application has been identified, the kernel uses only the Layer 4 header to match the traffic.
B. The IPS security profile is the only security option you can apply to the security policy with the action set to ACCEPT.
C. After IPS identifies the application, it adds an entry to a dynamic ISDB table.
D. FortiGate will drop all packets until the application can be identified.

**Answer:** D

**NEW QUESTION 35**
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

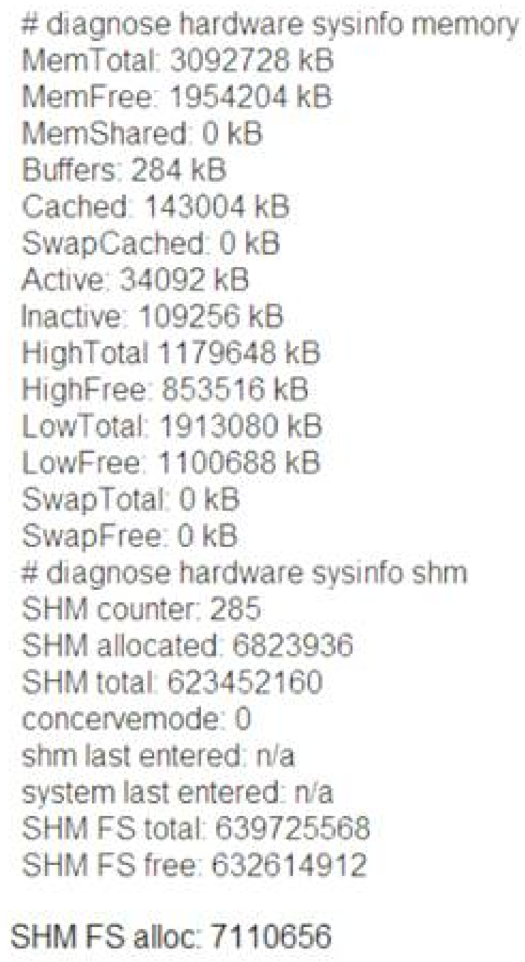
**NEW QUESTION 40**
The CLI command set intelligent-mode <enable | disable> controls the IPS engine’s adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

A. Determines the optimal number of IPS engines required based on system load.
B. Downloads signatures on demand from FDS based on scanning requirements.
C. Determines when it is secure enough to stop scanning session traffic.
D. Choose a matching algorithm based on available memory and the type of inspection being performed.

**Answer:** C

**Explanation:**
Configuring IPS intelligenceStarting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled the default and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate can quickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all known exploits. When disabled, the IPS engine scans every single byte.
config ips globalset intelligent-mode {enable|disable}end

**NEW QUESTION 44**
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 49**
View the IPS exit log, and then answer the question below.
# diagnose test application ipsmonitor 3 ipsengine exit log"
pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual
What is the status of IPS on this FortiGate?

A. IPS engine memory consumption has exceeded the model-specific predefined value.
B. IPS daemon experienced a crash.
C. There are communication problems between the IPS engine and the management database.
D. All IPS-related features have been disabled in FortiGate's configuration.

**Answer:** D

**Explanation:**
The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes.Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated:Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-releated features have been disabled)

**NEW QUESTION 54**
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

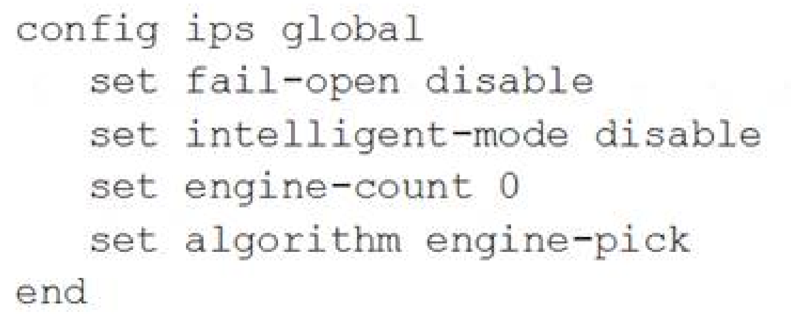
**NEW QUESTION 57**
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. Neighbor range
B. Route reflector
C. Next-hop-self
D. Neighbor group

**Answer:** B

**Explanation:**
Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routers learned from one peer to the other peers. If you configure route reflectors, you dont' need to create a full mesh IBGP network. All clients in a cluster only talck to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

**NEW QUESTION 62**
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
```

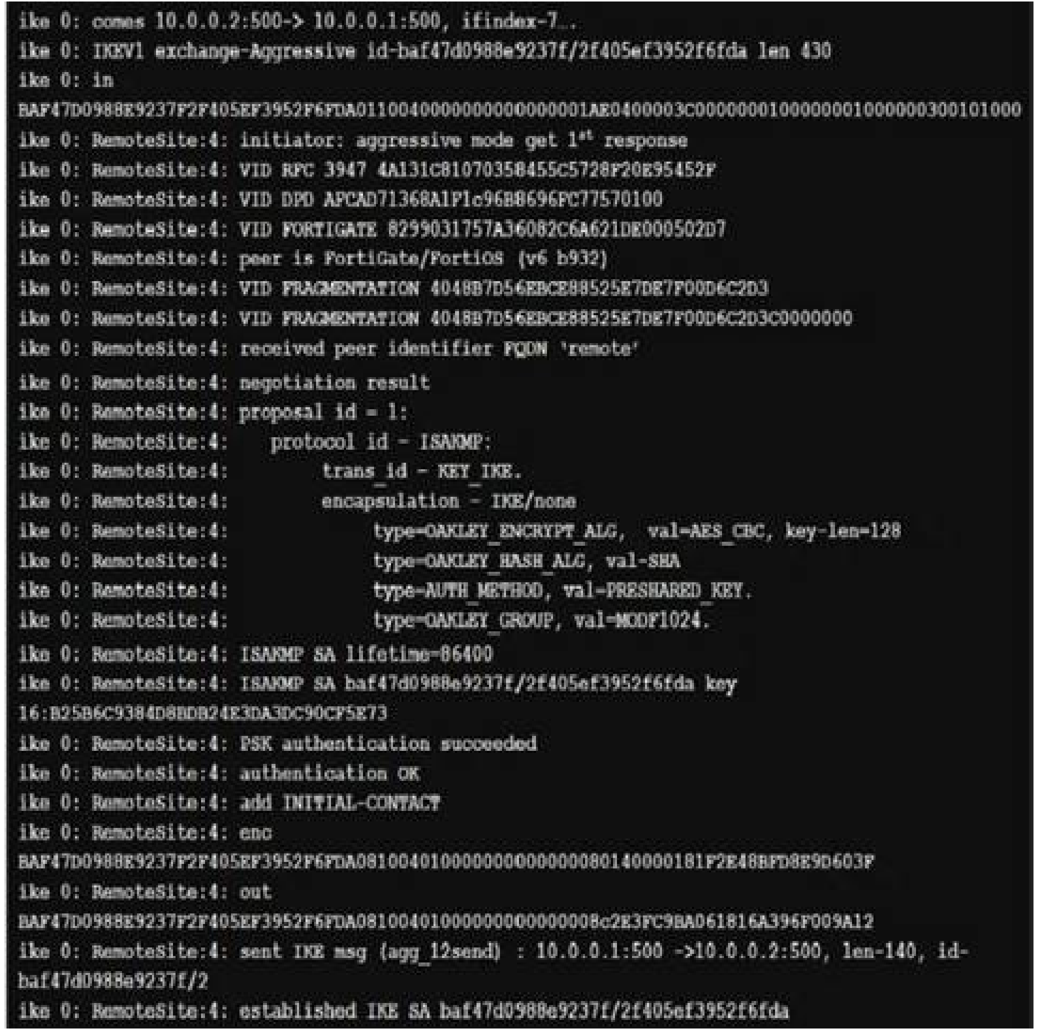
Which of the following statements is true regarding this configuration?

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.

**Answer:** A

**NEW QUESTION 66**

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
BAF47D0988E9237F2F405EF3952F6FDA011004000000000000000001AE0400003C000000010000000100000300101000
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 (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
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
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000000801400001 81F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

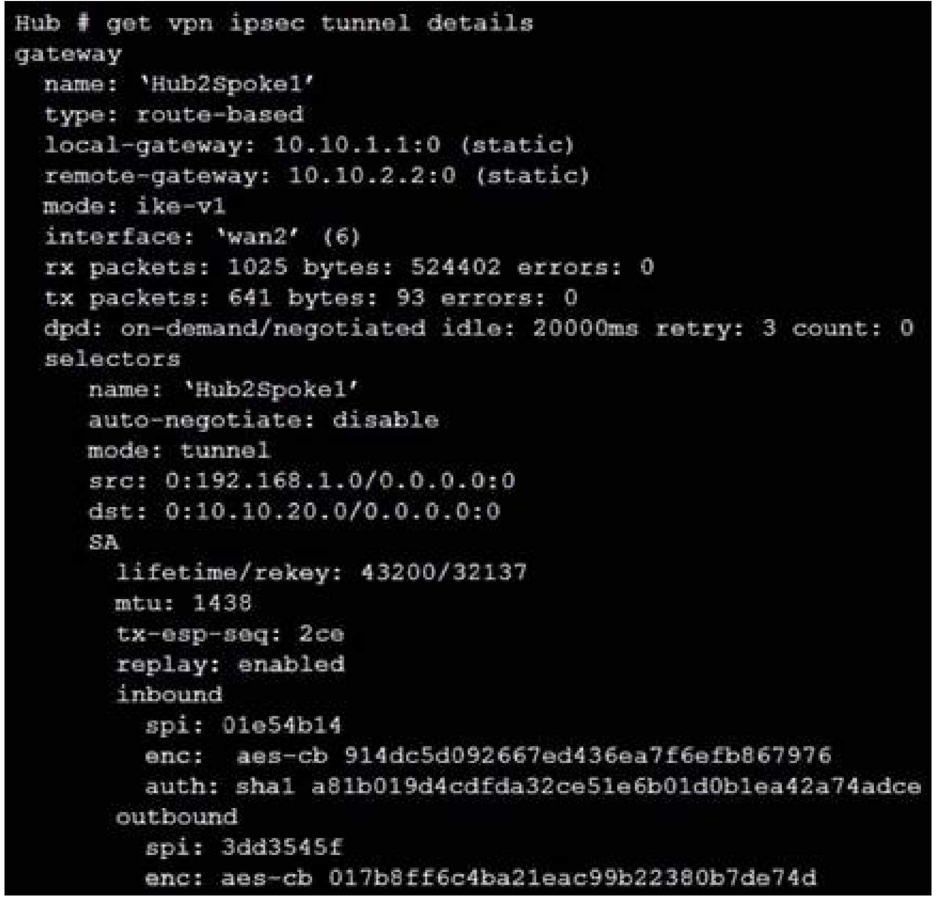
Which statements about this debug output are correct? (Choose two.)

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 67**

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
```

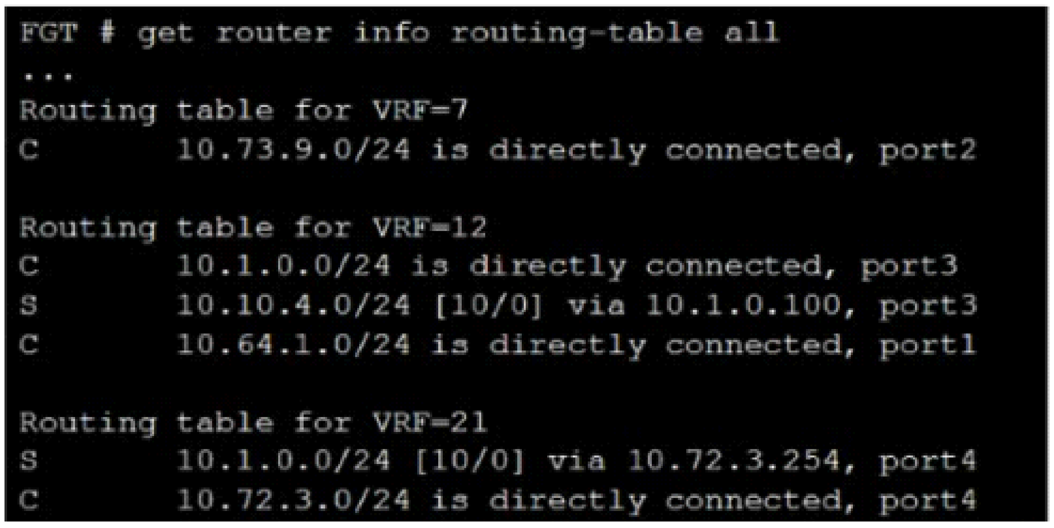
Based on the output, which two statements are correct? (Choose two.)

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 70**

Refer to the exhibit, which shows a partial routing table.



```
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
```

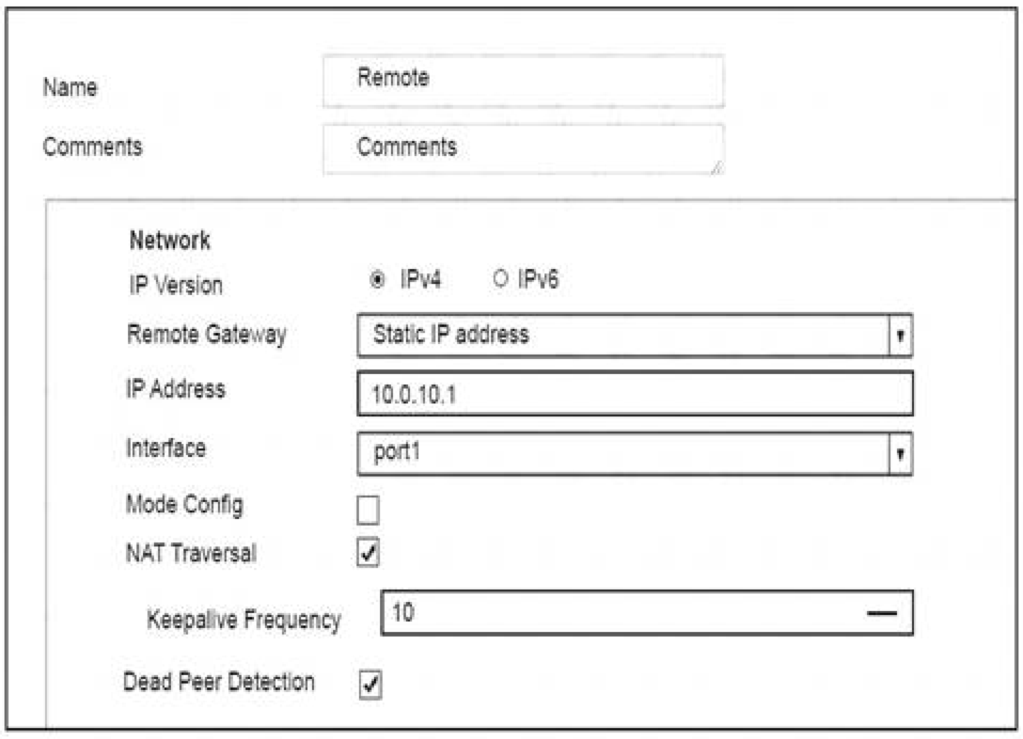
Assuming all the appropriate firewall policies are configured, which two pings will FortiGate route? (Choose two.)

A. Source IP address: 10.1.0.10. Destination IP address: 10.64.1.52
B. Source IPaddress: 10.72.3.52. Destination IP address: 10.1.0.254
C. Source IPaddress: 10.10.4.24, Destination IPaddress: 10.72.3.20
D. Source IPaddress: 10.73.9.10, Destination IPaddress: 10.72.3.15

**Answer:** AB

**NEW QUESTION 74**

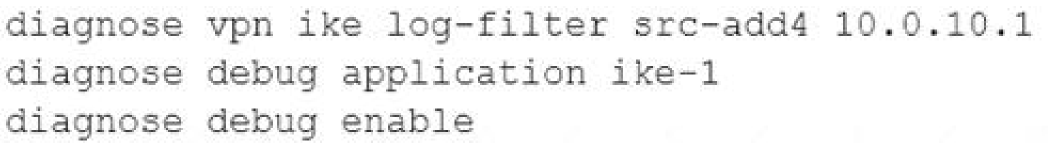
View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.



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
```

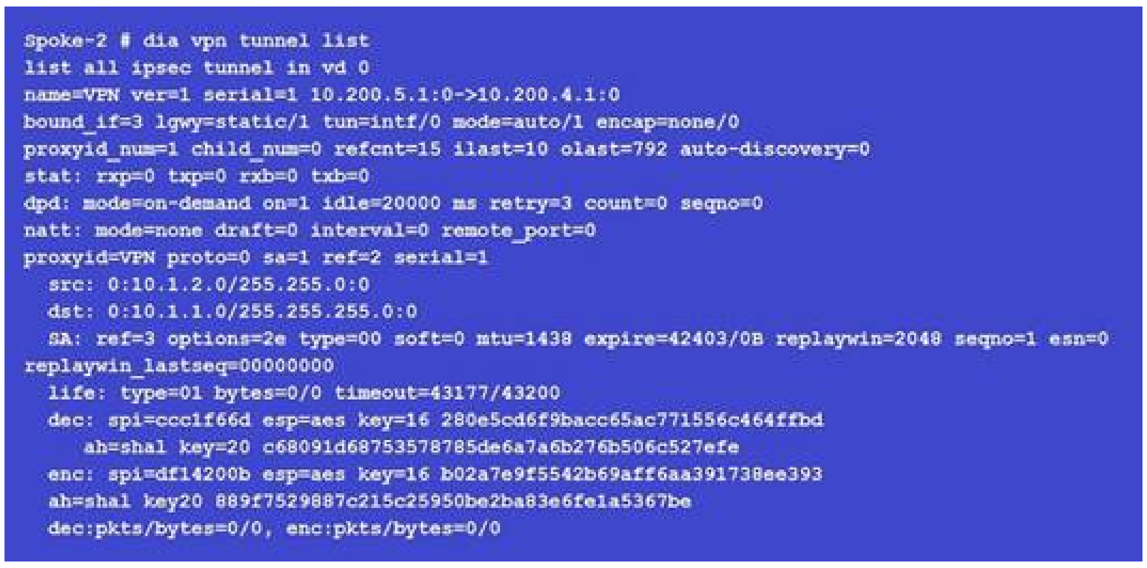
However, the IKE real time debug does not show any output. Why?

A. The debug output shows phases 1 and 2 negotiations onl
B. Once the tunnel is up, it does not show any more output.
C. The log-filter setting was set incorrectl
D. The VPN's traffic does not match this filter.
E. The debug shows only error message
F. If there is no output, then the tunnel is operating normally.
G. The debug output shows phase 1 negotiation onl
H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

**Answer:** B

**NEW QUESTION 79**

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



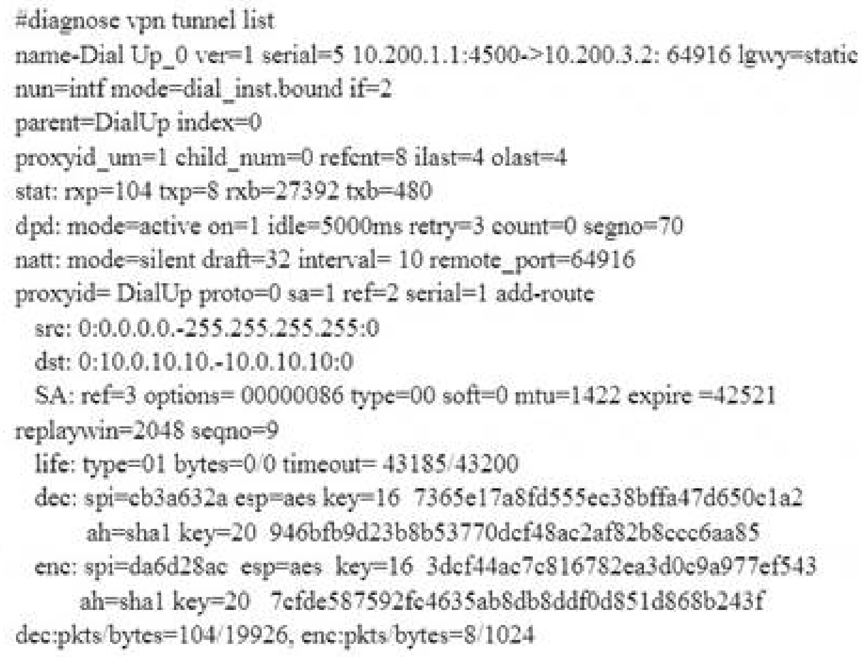
```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 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=shal key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=shal 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.

**Answer:** A

**NEW QUESTION 83**
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
```

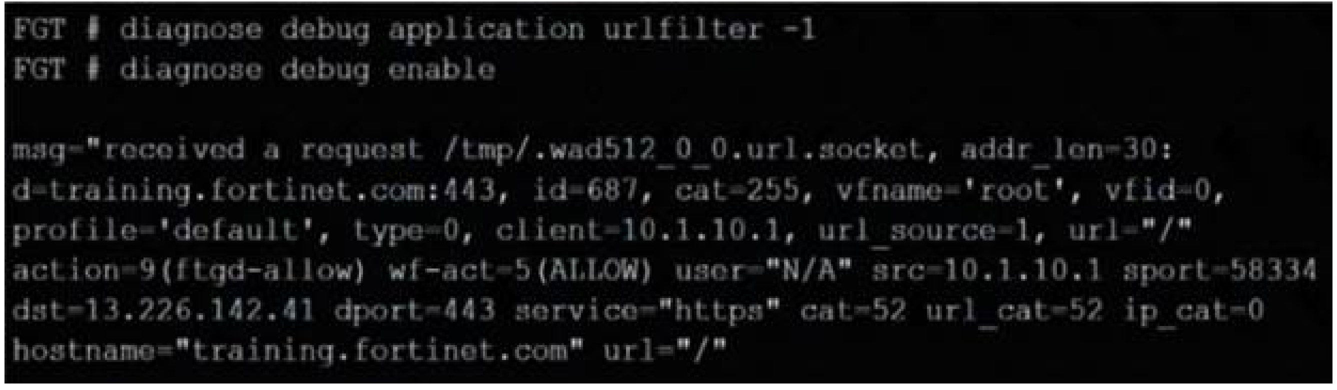
Which command can be used to sniffer the ESP traffic for the VPN DialUP_0?

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:** D

**Explanation:**
NAT-T is enabled. natt: mode=silentProtocol ESP is used. ESP is encapsulated in UDP port 4500 when NAT-T is enabled.
natt: mode=silent means IPSec is behind NAT (NAT traversal) https://kb.fortinet.com/kb/documentLink.do?externalID=FD48755

**NEW QUESTION 88**
View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?



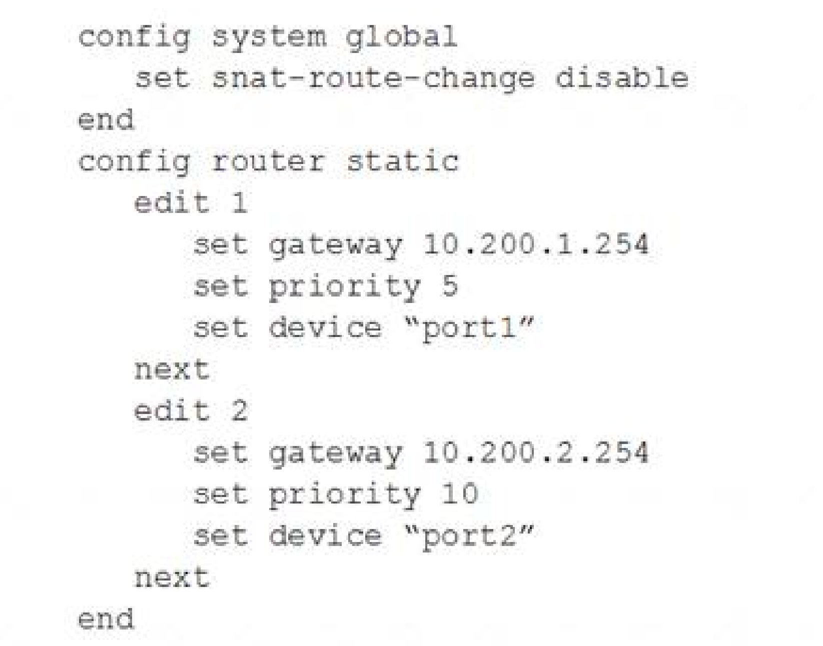
```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

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.

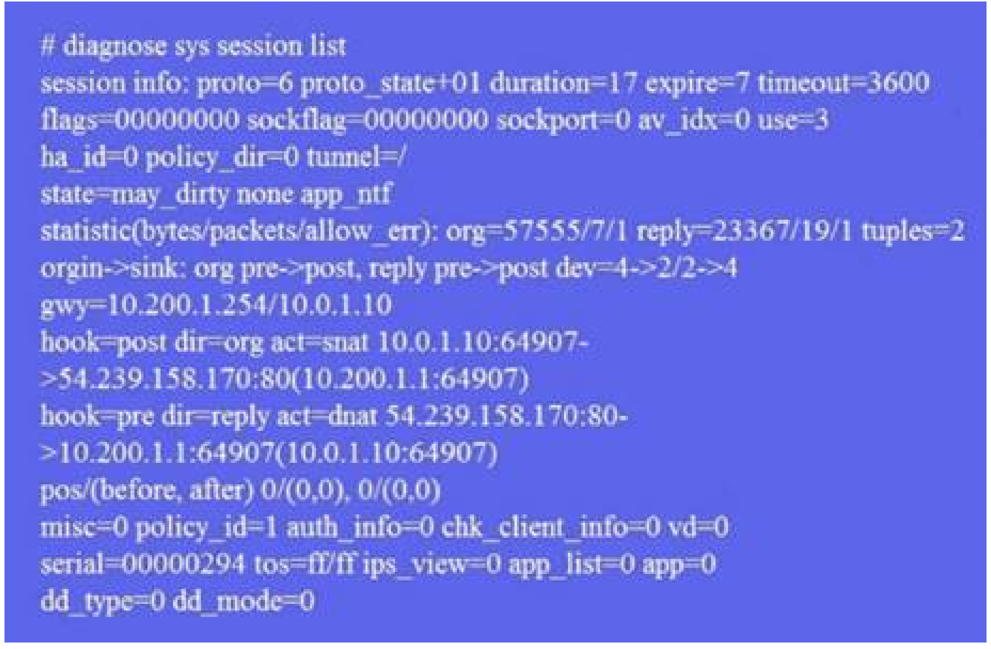
**Answer:** C

**NEW QUESTION 93**
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
   edit 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.

**Answer:** A

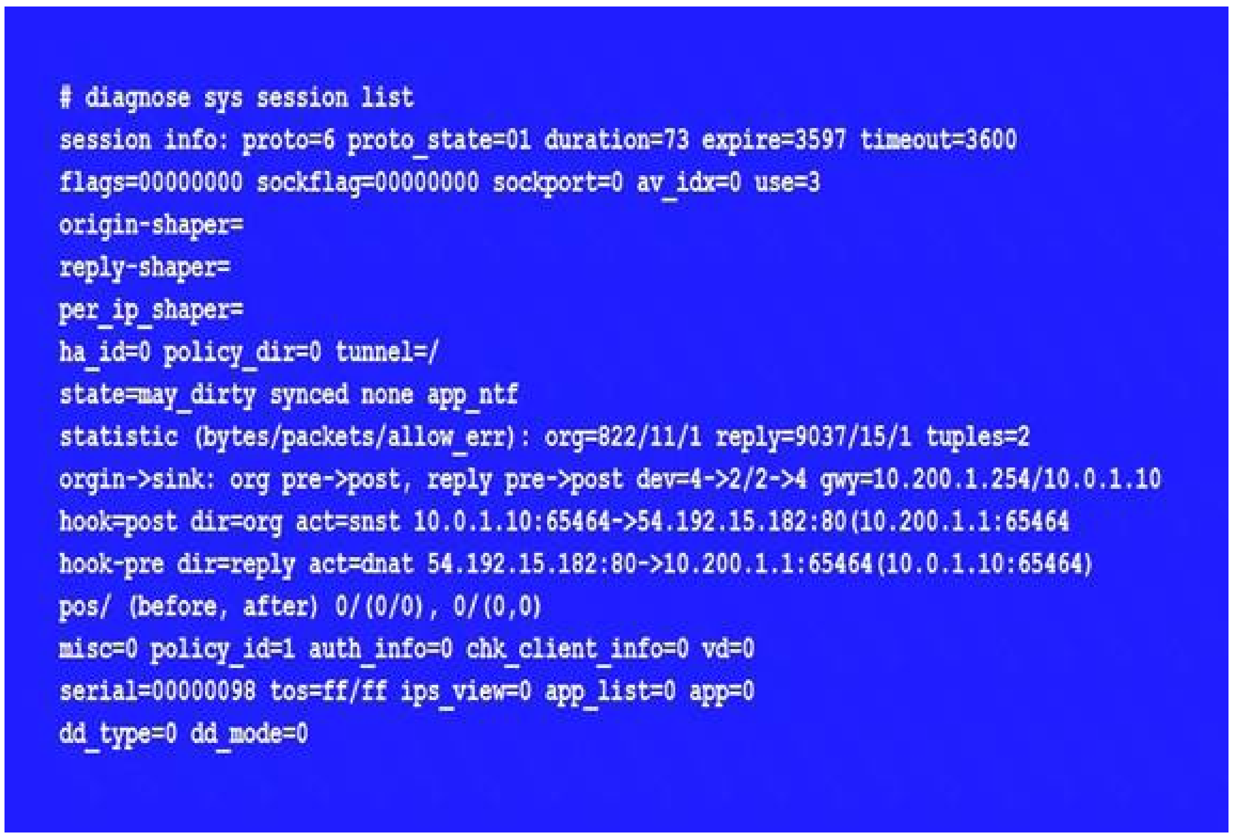
**Explanation:**
http://kb.fortinet.com/kb/documentLink.do?externalID=FD40943

**NEW QUESTION 98**
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 103**
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.



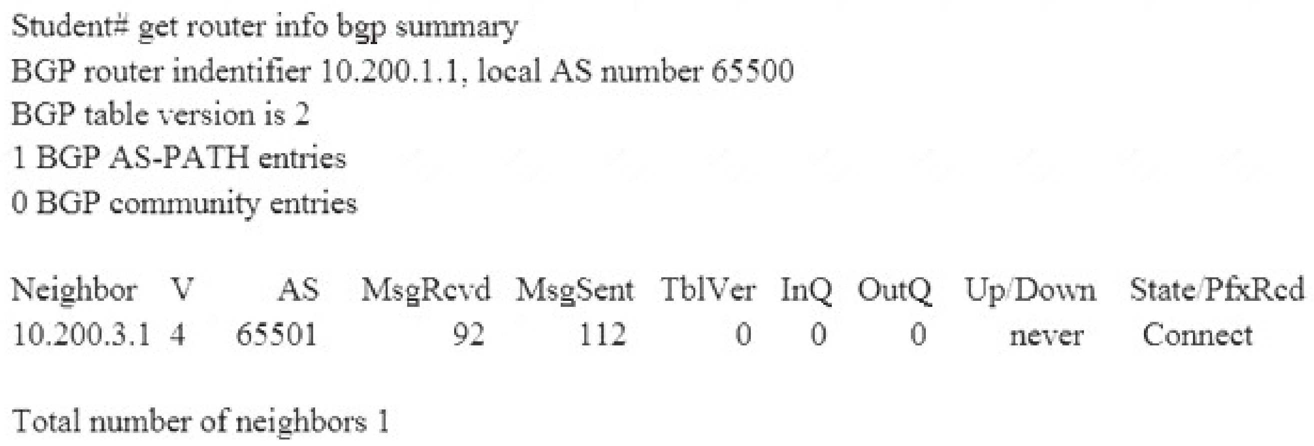
```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): 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 104**
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 109**
......