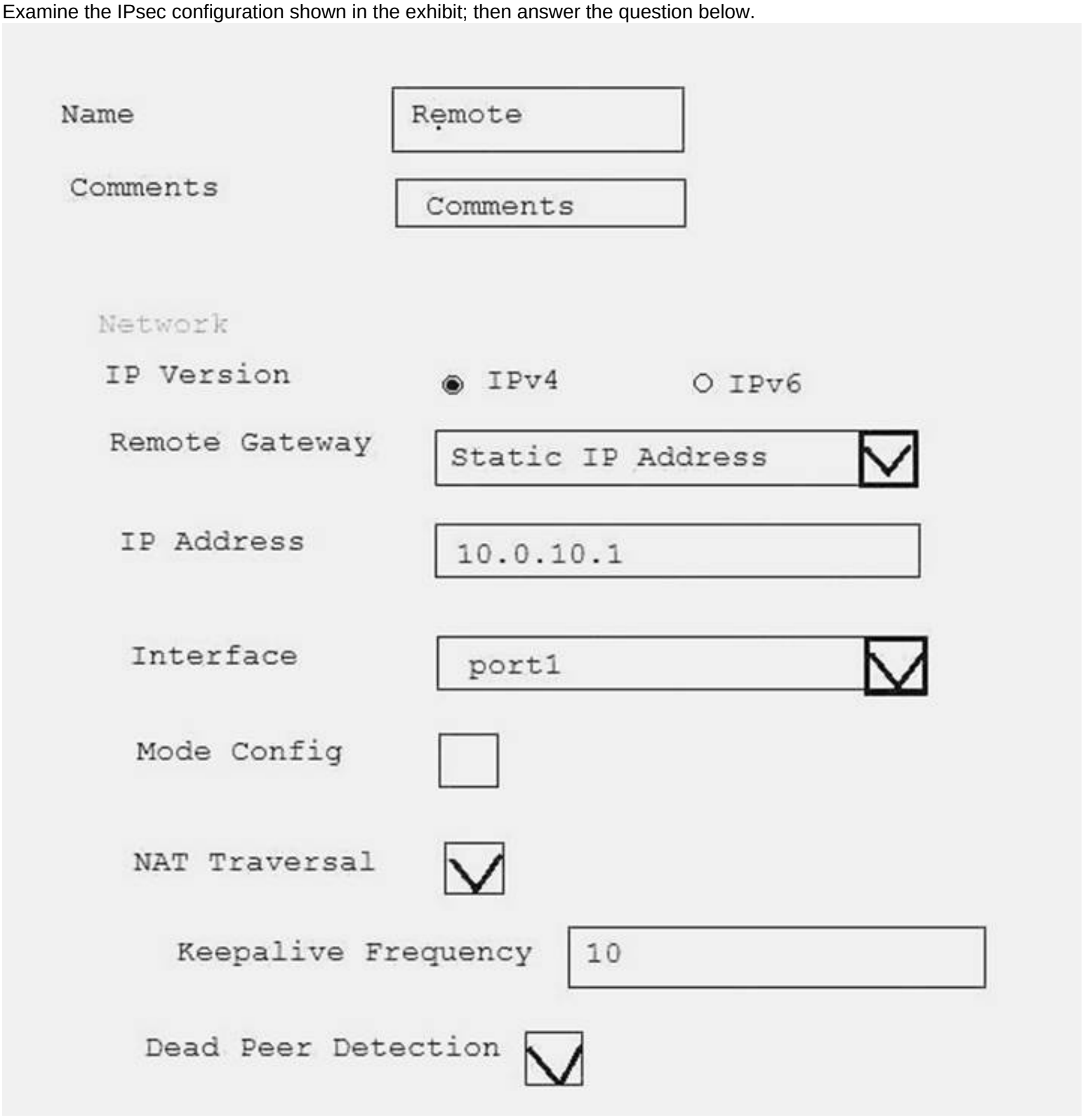
Fortinet

Exam Questions NSE7_EFW

NSE7 Enterprise Firewall - FortiOS 5.4

NEW QUESTION 1
Examine the IPsec configuration shown in the exhibit; then answer the question below.



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 outputonce 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 2
Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
B. SIP ALG supports SIP HA failover; SIP helper does not.
C. SIP ALG supports SIP over IPv6; SIP helper does not.
D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UD

Answer: BCD

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=Users, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "dc=trainingAD, dc=training, dc=lab"
     set password xxxxxxx
   next
end
```

The administrator executed the 'dsquery' command in the Windows LDAp server 10.0.1.10, and got the following output:
>dsquery user –samid administrator
"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.
B. username.
C. password.
D. d

Answer: A

NEW QUESTION 4
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy use
E. The limit CAN be modified by the administrator.
F. FortiGate limits the number of workstations that authenticate using the same web proxy user credential
G. This limit CANNOT be modified by the administrator.

Answer: C

NEW QUESTION 5
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 liv

Answer: A

NEW QUESTION 6
An administrator is running the following sniffer in a FortiGate:
diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

A. Ethernet headers.
B. IP payload.
C. IP headers.
D. Port name

Answer: BC

NEW QUESTION 7
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 technolog

Answer: C

NEW QUESTION 8
Examine the output of the 'get router info bgp summary' command shown in the exhibit; 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 statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.
B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixe

Answer: AC

NEW QUESTION 9
Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
……
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn't match the sniffer filter.
B. Number of total packets dropped by the FortiGate.
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
D. Number of packets that matched the sniffer filter but could not be captured by the sniffe

Answer: C

NEW QUESTION 10
An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

A. Router ID.
B. OSPF interface area.
C. OSPF interface cost.
D. OSPF interface MTU.
E. Interface subnet mas

Answer: BDE

NEW QUESTION 10
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; XAut

Answer: D

NEW QUESTION 15
When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.
B. The server requires more information from the user, such as the token code for two-factor authentication.
C. The user credentials are wrong.
D. The user account is not found in the serve

Answer: B

NEW QUESTION 17
The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

A. The CA cannot resolve the name of the workstation.
B. The FortiGate cannot resolve the name of the workstation.
C. The remote registry service is not running in the workstation 192.168.12.232.
D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

NEW QUESTION 21
Examine the output of the ‘get router info ospf neighbor’ command shown in the exhibit; then answer the question below.

```
# get router info ospf neighbor

OSPF process 0:
Neighbor ID   Pri   State           Dead Time   Address         Interface
0.0.0.69        1   Full/DR         00:00:32    10.126.0.69     wan1
0.0.0.117       1   Full/DROther    00:00:34    10.126.0.117    wan1
0.0.0.2         1   Full/ -         00:00:36    172.16.1.2      ToRemote
```

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

A. The interface ToRemote is OSPF network type point-to-point.
B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
C. The local FortiGate is the backup designated router for the wan1 network.
D. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.

Answer: AC

NEW QUESTION 23
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 mod

Answer: AD

NEW QUESTION 26
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 configuratio

Answer: A

NEW QUESTION 27
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. nd

Answer: C

NEW QUESTION 31
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: ….: 75: responder: aggressive mode get 1st message…
…
ike 0: ….:76: incoming proposal:
ike 0: ….:76: proposal id = 0:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id = KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: my proposal, gw Remote:
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val= PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val =MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP1536.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: ….:76: no SA proposal chosen
```

Why didn’t the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.
B. The remote gateway’s Phase-2 configuration does not match the local gateway’s phase-2configuration.
C. The remote gateway’s Phase-1 configuration does not match the local gateway’s phase-1 configuration.
D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mod

Answer: B

NEW QUESTION 33
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 34
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 handshak

Answer: AD

NEW QUESTION 36
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
#dia hardware sysinfo shm
SHM counter:            150
SHM allocated:            0
SHM total:       625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:  641236992
SHM FS free:   641208320
SHM FS avail:  641208320
SHM FS alloc:      28672
```

What statement is correct about this FortiGate?

A. It is currently in system conserve mode because of high CPU usage.
B. It is currently in FD conserve mode.
C. It is currently in kernel conserve mode because of high memory usage.
D. It is currently in system conserve mode because of high memory usag

Answer: D

NEW QUESTION 40
Which of the following tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Preview pending configuration changes for managed devices.
B. Add devices to FortiManager.
C. Import policy packages from managed devices.
D. Install configuration changes to managed devices.
E. Import interface mappings from managed device

Answer: BD

NEW QUESTION 43
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 configuratio

Answer: B

NEW QUESTION 44
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 inspectio

Answer: B

NEW QUESTION 48
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.

Answer: A

NEW QUESTION 51
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Reg received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which of the following statements about the exhibit are true? (Choose two.)

A. In the network on port4, two OSPF routers are down.
B. Port4 is connected to the OSPF backbone area.
C. The local FortiGate's OSPF router ID is 0.0.0.4
D. The local FortiGate has been elected as the OSPF backup designated route

Answer: BC

NEW QUESTION 56
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 58
View the exhibit, which contains the output of a real-time debug, and then answer the question below.

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

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache.   URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

A. This web request was inspected using the root web filter profile.
B. FortiGate found the requested URL in its local cache.
C. The requested URL belongs to category ID 52.
D. The web request was allowed by FortiGat

Answer: BC

NEW QUESTION 60
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
BAF47D0988E9237F2F405EF3952F6FDA011004000000000000001AE0400003C00000001000000010 00000300101000
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
BAF47D0988E9237F405EF3952F6FDA08100401000000000000000080140000181F2E48BFD8E9D603F
ike 0:RemoteSite:4: out BAF47D0988E9237F405EF3952F6FDA08100401000000000000000008C2E3FC9BA061816A396F009A12
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 I

Answer: BD

NEW QUESTION 63
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 applicatio

Answer: BC

NEW QUESTION 66
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 67
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 68
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 sessio

Answer: D

NEW QUESTION 70
View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
# diagnose debug rating
Locale          : english
License         : Contract
Expiration      : Thu Sep 28 17:00:00 20xx
-=- Server List (Thu Apr 19 10:41:32 20xx) -=-
IP                Weight  RTT  Flags  TZ  Packets  Curr Lost  Total Lost
64.26.151.37      10      45          -5  262432   0          846
64.26.151.35      10      46          -5  329072   0          6806
66.117.56.37      10      75          -5  71638    0          275
65.210.95.240     20      71          -8  36875    0          92
209.222.147.36    20      103    DI   -8  34784    0          1070
208.91.112.194    20      107    D    -8  35170    0          1533
96.45.33.65       60      144         0   33728    0          120
80.85.69.41       71      226         1   33797    0          192
62.209.40.74      150     97          9   33754    0          145
121.111.236.179   45      44     F    -5  26410    26226      26227
```

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

A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
B. Servers with the D flag are considered to be down.
C. Servers with a negative TZ value are experiencing a service outage.
D. FortiGate used 209.222.147.3 as the initial server to validate its contrac

Answer: CD

NEW QUESTION 75
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: D

NEW QUESTION 80
An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#    edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#    next
# end
```

Why didn't the script make any changes to the managed device?

A. Commands that start with the # sign are not executed.
B. CLI scripts will add objects only if they are referenced by policies.
C. Incomplete commands are ignored in CLI scripts.
D. Static routes can only be added using TCL script

Answer: B

NEW QUESTION 83
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

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

Answer: B

NEW QUESTION 86
View the exhibit, which contains the partial output of an IKE real time debug, and then answer the question below.

```
ike 0:9268ab9dea63aa3/0000000000000000:591: responder: main mode get 1st message…
…
ike 0:9268ab9dea63aa3/0000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:       trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:       encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id=0:
ike 0:9268ab9dea63aa3/0000000000000000:591:   protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:      trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:      encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISA KMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: my proposal, gw VPN:
ike 0:9268ab9dea63aa3/0000000000000000:591:   proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:       trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:       encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:           type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:           type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:           type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:           type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:    protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:      trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:      encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:    protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:      trans_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:      encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:         type= OAKLEY_ENCRYPT_ALG, val =AES-CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
```

The administrator does not have access to the remote gateway. Based on the debug output, what configuration changes can the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. Change phase 1 encryption to AESCBC and authentication to SHA128.
B. Change phase 1 encryption to 3DES and authentication to CBC.
C. Change phase 1 encryption to AES128 and authentication to SHA512.
D. Change phase 1 encryption to 3DES and authentication to SHA256.

Answer: C

NEW QUESTION 89
View the exhibit, which contains the output of a diagnose command, and the answer the question below.

```
# diagnose debug rating
Locale       : English
License      : Contract
Expiration   : Thu Sep 28 17:00:00 20XX
-=- Server List (Thu APR 19 10:41:32 20XX) -=-
IP               Weight   RTT   Flags   TZ   Packets  Curr Lost  Total Lost
64.26.151.37     10       45            -5    262432  0           846
64.26.151.35     10       46            -5    329072  0           6806
66.117.56.37     10       75            -5    71638   0           275
66.210.95.240    20       71            -8    36875   0           92
209.222.147.36   20       103    DI     -8    34784   0           1070
208.91.112.194   20       107    D      -8    35170   0           1533
96.45.33.65      60       144           0     33728   0           120
80.85.69.41      71       226           1     33797   0           192
62.209.40.74     150      97            9     33754   0           145
121.111.236.179  45       44     F      -5    26410   26226       26227
```

Which statements are true regarding the Weight value?

A. Its initial value is calculated based on the round trip delay (RTT).
B. Its initial value is statically set to 10.
C. Its value is incremented with each packet lost.
D. It determines which FortiGuard server is used for license validatio

Answer: C

NEW QUESTION 92
In which of the following states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.
B. A TCP session waiting for FIN ACK.
C. A UDP session with packets sent and received.
D. A UDP session with only one packet receive

Answer: BC

NEW QUESTION 96
View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: A

NEW QUESTION 98
Which of the following statements are true about FortiManager when it is deployed as a local FDS? (Choose two.)

A. Caches available firmware updates for unmanaged devices.
B. Can be configured as an update server, or a rating server, but not both.
C. Supports rating requests from both managed and unmanaged devices.
D. Provides VM license validation service

Answer: AD

NEW QUESTION 99
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 100
What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

A. Reduce the session time to live.
B. Increase the TCP session timers.
C. Increase the FortiGuard cache time to live.
D. Reduce the maximum file size to inspec

Answer: AD

NEW QUESTION 101
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.

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

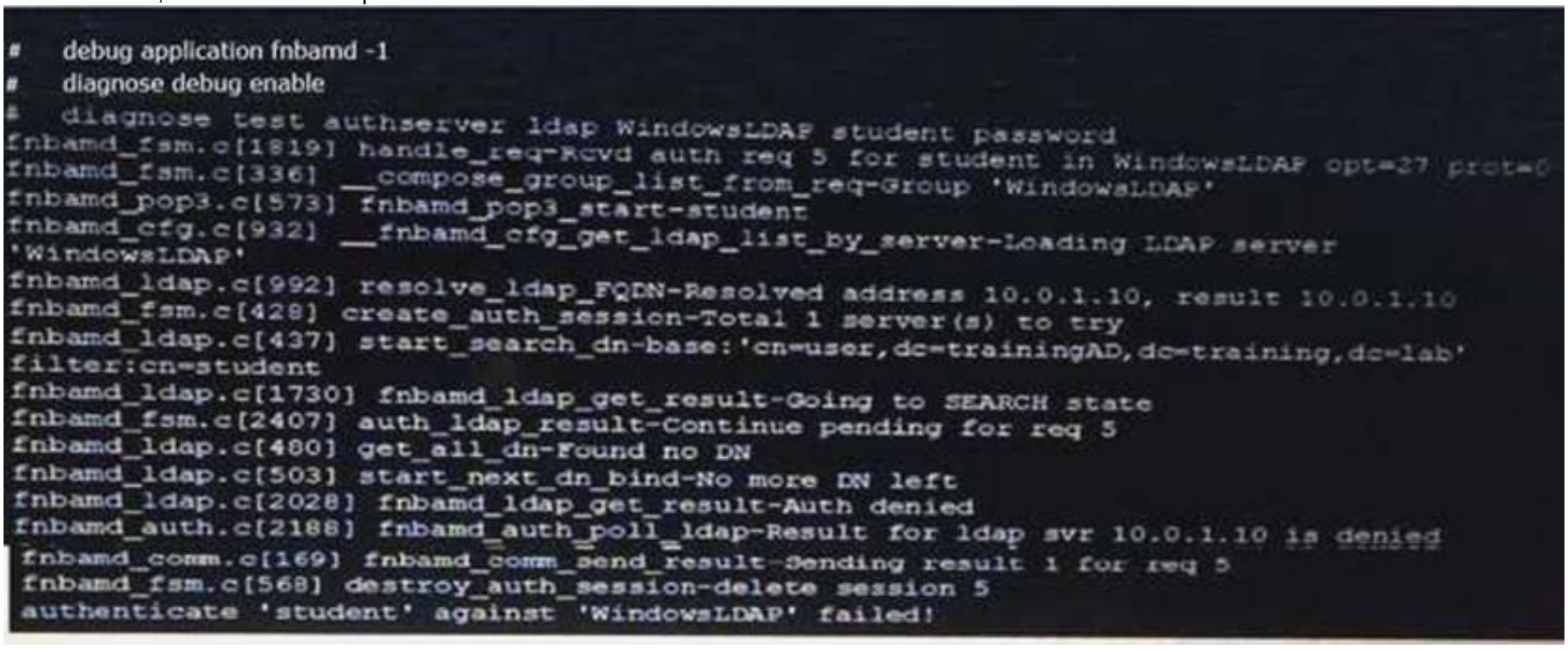
Answer: C

NEW QUESTION 102
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 107
An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.



A. User student is not found in the LDAP server.
B. User student is using a wrong password.
C. The FortiGate has been configured with the wrong password for the LDAP administrator.
D. The FortiGate has been configured with the wrong authentication schem

Answer: A

NEW QUESTION 112
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 116
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_EFW Practice Exam Features:

* NSE7_EFW Questions and Answers Updated Frequently

* NSE7_EFW Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year