Fortinet

Exam Questions NSE7_EFW-6.2

Fortinet NSE 7 - Enterprise Firewall 6.2

NEW QUESTION 1
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 2
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 thedebug 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 3
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# diagnose hardware sysinfo conserve
memory conserve mode:                    on
total RAM:                               3040 MB
memory used:                             2706 MB 89% of total RAM
Memory freeable:                          334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:               2675 MB 88% of total RAM
memory used threshold green:             2492 MB 82% of total RAM
```

Which one of the following statements about this FortiGate is correct?

A. It is currently in system conserve mode because of high CPU usage.
B. It is currently in extreme conserve mode because of high memory usage.
C. It is currently in proxy conserve mode because of high memory usage.
D. It is currently in memory conserve mode because of high memory usage.

Answer: D

NEW QUESTION 4
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 5
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 istrue 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 explicitproxy-based inspection.

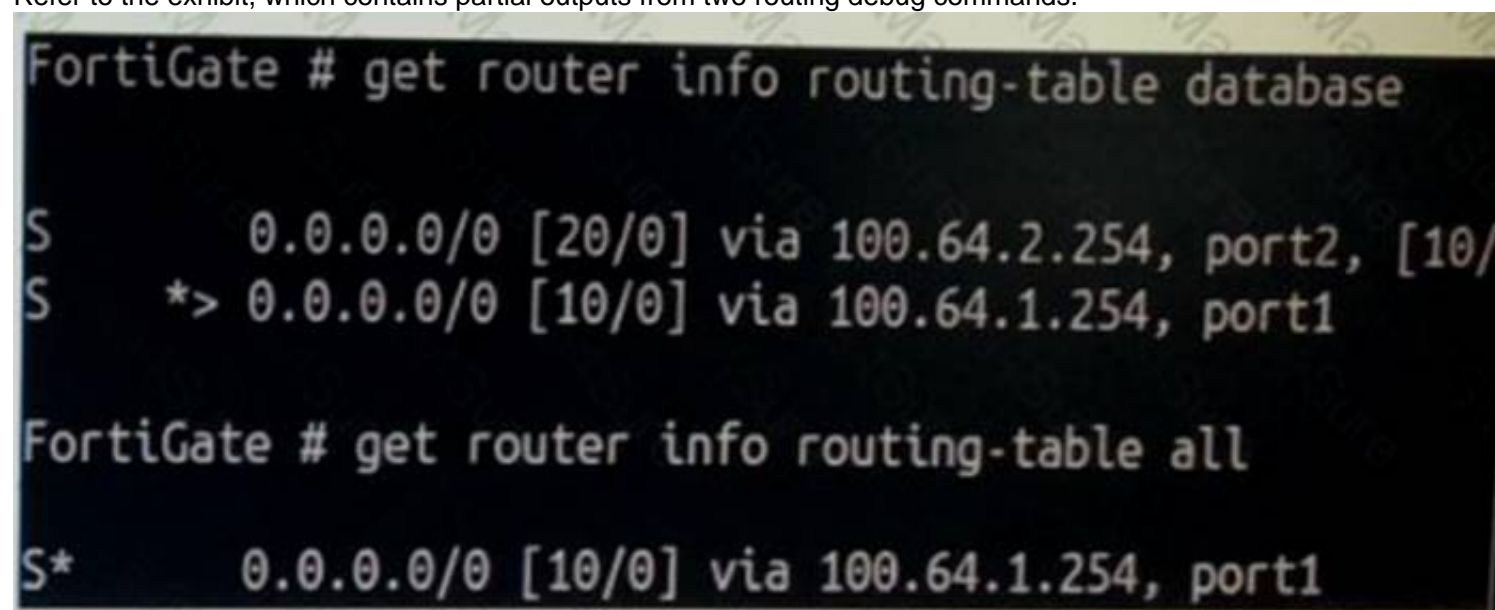**Answer:** A

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 6
Refer to the exhibit, which contains partial outputs from two routing debug commands.

```
FortiGate # get router info routing-table database

S       0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/
S    *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command's output?

A. It has a higher priority value than the default route using port1.
B. It isdisabled in the FortiGate configuration.

C. It has a lower priority value than the default route using port1.
D. It has a higher distance than the default route using port1.

Answer: D

NEW QUESTION 7
View the exhibit, which contains the partial output of an IKE real time debug, and then answer thequestion 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 1encryption 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 8
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: A

NEW QUESTION 9
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 10
Examine the output of the 'get router info ospf interface' command shown in the exhibit; 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 statements are true regarding the above output? (Choose two.)

A. The port4 interface is connected to the OSPF backbone area.
B. The local FortiGate has been elected as theOSPF backup designated router.
C. There are at least 5 OSPF routers connected to the port4 network.
D. Two OSPF routers are down in the port4 network.

Answer: AC

Explanation:
on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So ourFG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DRother (not down).

NEW QUESTION 10
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 11
A FortiGate device has thefollowing 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. dn.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

NEW QUESTION 15
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 16
Examine the output from the 'diagnose vpn tunnel list' command shown inthe 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 seqno=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 'host10.0.10.10'
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.

NEW QUESTION 19
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. IKEmode 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-2 configuration.
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 mode.

Answer: C

NEW QUESTION 22
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 mask.

Answer: BDE

NEW QUESTION 24
View the exhibit, which contains the output of diagnose syssession 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. Theinspection of this session has been offloaded to the slave unit.
D. This session cannot be synced with the slave unit.

Answer: B

NEW QUESTION 26
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 27
A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878   n_dns_fails= 2   n_dns_timeout=875
n_dns_success=0

n_snd_retries=0   n_snd_fails=0  n_snd_success=0  n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

A. The connectivity between the FortiGate unit and the DNS server.
B. The connectivity between the client workstations and the DNS server.
C. That DNS traffic from client workstations isallowed by the explicit web proxy policies.
D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

NEW QUESTION 31
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 32
In which two 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 received.

Answer: AD

NEW QUESTION 37
An administrator has decreased all the TCP session timers to optimize theFortiGate 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/commo
n/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, asession 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 41
An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit.The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failoveroccurs.
B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
C. Sends a link failed signal to all connected devices.
D. Disables all the non-heartbeat interfaces inall the HA members for two seconds after a failover.

Answer: A

NEW QUESTION 46
View the exhibit, which contains the partial output of a diagnose command, and then answer thequestion 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 49
Which real time debug should an administrator enable to troubleshoot RADIUSauthentication 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: B

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838

NEW QUESTION 52
View the global IPSconfiguration, 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 57
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 defaultroute using port1.
D. It is disabled in the FortiGate configuration.

Answer: C

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

NEW QUESTION 60
Examine the output fromthe BGP real time debug shown in the exhibit, then the answer the question below:

```
#    diagnose ip router bgp all enable
#    diagnose ip router bgp level info
#    diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byt
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

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

A. BGP peers have successfully interchangedOpenandKeepalivemessages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer isOpenConfirm.
D. The state of the remote BGP peer will go toConnectafter it confirms the received prefixes.

Answer: AB

NEW QUESTION 64
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 thequestion below.

```
#    debug application fnbamd -1
#    diagnose debug enable
#    diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_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[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
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 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

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 schema.

Answer: A

NEW QUESTION 67
When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the usercredentials 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 server.

Answer: B

NEW QUESTION 68
View the exhibit, which contains the output of areal-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 localcache.
C. The requested URL belongs to category ID 52.
D. The web request was allowed by FortiGate.

Answer: BC

NEW QUESTION 71
View the central managementconfiguration shown in the exhibit, and then answer the question below.

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

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

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

Answer: B

NEW QUESTION 75
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. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.
B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.
C. Session would be deleted, so the client would need to start a new session.
D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Answer: A

NEW QUESTION 77
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

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548

NEW QUESTION 78
View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
     diagnose sys session list expectation

session info: proto=6 proto_state-00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-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
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What statements are correctregarding the output? (Choose two.)

A. This is an expected session created by a session helper.
B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
C. Traffic in the originaldirection (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
D. This is an expected session created by an application control profile.

Answer: AC

NEW QUESTION 80
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 to20, 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 fromboth 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 83
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. IPheaders.
D. Port names.

Answer: BC

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=11186

NEW QUESTION 84
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. Itwas created by a session helper or ALG.

Answer: D

NEW QUESTION 87
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 91
What does the dirty flag mean in a FortiGate session?

A. Traffic has been blocked by the antivirus inspection.
B. The next packet must be re-evaluated against the firewall policies.
C. The session must be removed from the former primaryunit after an HA failover.
D. Traffic has been identified as from an application that is not allowed.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1

NEW QUESTION 92
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
```

Whichstatements 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

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

NEW QUESTION 94
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 theround 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 validation.

Answer: C

NEW QUESTION 96
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-Req 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 onport4, 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 router.

Answer: BC

NEW QUESTION 97
Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-miltipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

TheBGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

A. Enable the redistribution of connected routers into BGP.
B. Enable the redistribution of static routers into BGP.
C. Disable the setting network-import-check.
D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 98
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 103
Which of thefollowing 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: CD

Explanation:
Application layer test commands don't display info in real time, but they do show statistics and configuration info about a feature or process. You canalso use some of these commands to restart a process or execute a change in its operation.

NEW QUESTION 104
......

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-6.2 Practice Exam Features:

* NSE7_EFW-6.2 Questions and Answers Updated Frequently

* NSE7_EFW-6.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-6.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-6.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-6.2 Practice Test Here](https://www.certshared.com/exam/NSE7_EFW-6.2/)