Fortinet.Premium.NSE7.by.VCEplus.60q

Number: NSE7 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 2.5

Exam Code: NSE7
Exam Name: NSE7 Enterprise Firewall - FortiOS 5.4
Certification Provider: Fortinet
Corresponding Certification: NSE7
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-nse7-fortinet/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in NSE7 exam products and you get latest questions. We strive to deliver the best NSE7 exam product for top grades in your first attempt.

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

QUESTION 1
what conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. IP addresses are in the same subnet.
B. Hello and dead intervals match.
C. OSPF IP MTUs match.
D. OSPF peer IDs match.
E. OSPF costs match.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.
B. Policy monitor.
C. Logs.
D. Crashlogs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor   V     AS   MsgRcvd   MsgSent   TblVer   InQ   OutQ   Up/Down   State/PfxRcd
10.200.3.1 4   65501        92       112        0     0      0     never    Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
B. The TCP session for the BGP connection to 10.200.3.1 is down.
C. The local peer has received the BGP prefixed from the remote peer
D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
An administrator has enabled HA session synchronization in a HA cluster with two members, which flag is added to a primary unit's session to indicate that it has been synchronized to the secondary unit?

A. redir.
B. dirty.
C. synced
D. nds.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
which of the following conditions must be met for a static route to be active in the routing table? (Choose three)

A. The next-hop IP address is Up.
B. There is no other route, to the same destination, with a higher distance.
C. The link health monitor (if configured) is up
D. The next-hop IP address belongs to one of the outgoing interface subnets.
E. The outgoing interface is up.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:  comes 10.0.0.2:500->10.0.0.1:500, ifindex=7....
ike 0:  IKEv1 exchange=Aggressive id=baf47d0988e9237f/2f405ef3952f6fda len=430
ike 0:  in BAF47D0988E9237F2F405EF3952F6FDA011004000000000000000001AE0400003C000000010000000100000030010100 0
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 IP sec pear ID.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Examine the following partial outputs from two routing debug commands, then answer the question below:

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

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

A. It has a lower priority than the default route using port1.
B. It has a higher priority than the default route using port1.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
which real time dehug should an administrator enable to troubleshoot RADIUS authentication problems?

A. Diagnose debug application radius -1.
B. Diagnose debug application fnbamd -1.
C. Diagnose authd console -log enable.
D. Diagnose radius console -log enable.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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'

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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. Thesessionwould remainin the sessiontable, and its traffic would still egress from port 1.
B. Thesessionwould remainin the sessiontable, but its traffic would now egress from both port 1and port2
C. Thesessionwould remainin the sessiontable, and its traffic would start to egress from port2.
D. The session would be deleted, so the client would need to start a new session.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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. dn.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below

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


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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
when using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter weh requests when the browser client does not provide the server name indication (SNI)?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
View the central management configuration 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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; SIR helper does not
C. SIP ALG supports SIP over IPv6; SIR 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 UDP.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
View the exhibit, which contains the partial output of a diagnose command, and then answer the question below:

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
     ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=sha1 key20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. Anti-reply is enabled.
B. DPD is disabled.
C. Quick mode selectors are disabled.
D. Remote gateway IP is 10.200.5.1.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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 server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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 prefixes.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer, if the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any 'udp port 500'
B. diagnose sniffer packet any ‘udp port 4500'
C. diagnose sniffer packet any 'esp'
D. diagnose sniffer packet any ‘udp port 500 or udp port 4500'

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
what global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

A. av-failopen
B. mem-failopen
C. utm-failopen
D. ips-failopen

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
View the exhibit, which contains the output of a web diagnose command, and then answer the question below:

diagnose webfilter fortiguard statistics list

Raring Statistics:

DNS filures	:	273
DNS lookups	:	280
Data send failures	:	0
Data read failures	:	0
Wrong package type	:	0
Hash table miss	:	0
Unknown server	:	0
Incorrect CRC	:	0
Proxy requests failures	:	0
Request timeout	:	1
Total requests	:	2409
Requests to FortiGuard servers	:	1182
Server errored responses	:	0
Relayed rating	:	0
Invalid profile	:	0

diagnose webfilter fortiguard statistics list

Cache Statistics:

Maximum memory	:	0
Memory usage	:	0
Nodes	:	0
Leaves	:	0
Prefix nodes	:	0
Exact nodes	:	0
Requests	:	0
Misses	:	0
Hits	:	0
Prefix hits	:	0
Exact hits	:	0
No cache directives	:	0

Allowed	:	1021
Blocked	:	3909
Logged	:	3927
Blocked Errors	:	565
Allowed Errors	:	0
Monitors	:	0
Authenticates	:	0
Warnings	:	18
Ovrd request timeout	:	0
Ovrd send failures	:	0
Ovrd read failures	:	0
Ovrd errored responses	:	0
...		

Add after prefix	:	0
Invalid DB put	:	0
DB updates	:	0
Percent full	:	0%
Branches	:	0%
Leaves	:	0%
Prefix nodes	:	0%
Exact nodes	:	0%
Miss rate	:	0%
Hit rate	:	0%
Prefix hits	:	0%
Exact hits	:	0%

Which one of the following statements explains why the cache statistics are all zeros?

A. The administrator has reallocated the cache memory to a separate process.
B. There are no users making web requests.
C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

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

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

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

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


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

A. auto-discovery-sender

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit, than answer the question below:

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag= ·00000000 ·sockport=0 ·av_idx=0 ·use=3¶
origin-shaper=¶
reply-shaper=¶
per-ip_shaper=¶
ha_id=0 ·policy_dir=1 ·tunnel=/¶
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)¶
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 ·policy_id=1 ·auth_info=0 ·chk_client_info=0 ·vd=0
serial1=000000e9 ·tos=ff/ff ·ips_view=0 app_list=0 ·app=0
dd type=0 ·dd_mode=0¶
```


Which statement is true regarding the session in the exhibit?

A. It was created by the FortiGate kernel to allow push updates from FotiGuard
B. It is for management traffic terminating at the FortiGate.
C. It is for traffic originated from the FortiGate.
D. It was created by a session helper or ALG.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A FortiGate device has the following LDAP configuration:

```
config user ldap
   edit "WindowsLDAP"
     set server "10.0.1.10"
     set cnid "cn"
     set dn "cn=user, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
     set password xxxxx
   next
end
```


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

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


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

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference: