Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
Examine the output from the 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 interchanged Open and Keepalive messages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer is OpenConfirm.
D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 2
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 3
Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen
B. mem failopen
C. AV failopen
D. UTM failopen

Answer: AC

NEW QUESTION 4
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 5
Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # 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=100.64.1.254 dev=3(port1)
tab=254 vf=0 scope=0 type=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=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9(port3)


FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
                  [10/0] via 100.64.2.254, port2, [10/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.10.0/24 [10/0] via 10.1.0.1, port3
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

A. Set the priority of the static default route using port1 to 10. Most Voted
B. Set the priority of the static default route using port2 to 1.
C. Set preserve-session-route to enable.
D. Set snat-route-change to enable.

Answer: A

Explanation:
ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.
https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/25967/equal-cost-multi-path

NEW QUESTION 6
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:     protocol id = ISAKMP:
ike 0: Remotesite:3:          trans_id = KEY_IKE.
ike 0: Remotesite:3:          encapsulation = IKE/none.
ike 0: Remotesite:3:               type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:               type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:               type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:               type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

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

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

Answer: BC

NEW QUESTION 7
Refer to the exhibit, which shows a partial web filter profile configuration.

FortiGuard Category Based Filter

Name	Action
⊟ Bandwidth Consuming ⑥	
Freeware and Software Downloads	✔ Allow
File Sharing and Storage	⊘ Block

Static URL Filter

URL Filter 🔵

➕ Create New ✏ Edit 🗑 Delete | Search 🔍

URL	Type	Action	Status
*.dropbox.com	Wildcard	✔ Allow	✔ Enable

Content Filter 🔵

➕ Create New ✏ Edit 🗑 Delete

Pattern Type ⇕	Pattern ⇕	Language ⇕	Action ⇕	Status ⇕
Wildcard	*dropbox*	Western	⊖ Exempt	✔ Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

A. FortiGate will block the connection, based on the FortiGuard category based filter configuration.
B. FortiGate will block the connection as an invalid URL.
C. FortiGate will exempt the connection, based on the Web Content Filter configuration.
D. FortiGate will allow the connection, based on the URL Filter configuration.

Answer: A

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 351 url filter -> FortiGuard Web Filter -> Web Content Filter -> Advanced Filter Options Allow -> Block

NEW QUESTION 8
An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.
If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

A. diagnose sniffer packet any 'ah'
B. diagnose sniffer packet any 'ip proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'udp port 500'

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p. 443 Phase 2 : ESP => IP protocol 50
This command will capture any packets that use the IP protocol number 50, which is ESP (Encapsulating Security Payload). ESP is used to encrypt and authenticate the phase 2 traffic between two FortiGate device1s.

NEW QUESTION 9
Refer to the exhibit, which contains a CLI script configuration on FortiManager.

Script Name	Static Route
Comments	
	0/255
	0/255
Type	CLI Script ▼
Run script on	Remote FortiGate Directly (... ▼
Script details	# conf rout stat # edit 0 # set gateway 10.20.121.2 # set priority 20 # set device "wan1" # next # end

An administrator configured the CLI script on FortiManager, but the script failed to apply any changes to the managed device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two.)

A. Static routes can be added using only TCL scripts.
B. The commands that start with the # sign did not run.
C. CLI scripts must start with #!.
D. Incomplete commands can cause CLI scripts to fail.

Answer: BD

Explanation:
ref CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not "#!" as it is for Tcl scripts.
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

NEW QUESTION 10
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.

```
#    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 10
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 contract.

Answer: AD

Explanation:
* A – because flag is Failed so fortigate will check if server is available every 15 minD-state is I , contact to validate contract info

NEW QUESTION 12
Refer to the exhibit, which contains the output of diagnose sys session list.

```
# 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=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
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=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(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 about the output is true?

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

Answer: C

NEW QUESTION 16
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 usage.

Answer: D

NEW QUESTION 19
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. route-reflector enable
B. route-reflector-server enable
C. route-reflector-client enable
D. route-reflector-peer enable

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/572620/config-router-bgp set route-reflector-client [enable|disable]

NEW QUESTION 22
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phase1 -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 phase1 name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

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

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

What is causing the IPsec problem in the phase 1 ?

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

Answer: C

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

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

Answer: AD

NEW QUESTION 28
Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 655
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS      MsgRcvd MsgSent     TblVe
10.200.3.1      4 65501      92      1756        0

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router has a different AS number than the remote peer.
B. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the openConfirm yet.
C. The local router initiated the BGP session to 10.200.3.1 but did not receive a response.
D. The router 10.200.3.1 has authentication configured for BGP and the local router does not.

Answer: C

NEW QUESTION 29
An administrator has created a VPN community within VPN Manager on FortiManager. They also added gateways to the VPN community and are now trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces are not listed as available options.
What step must the administrator take to resolve this issue?

A. Install the VPN community and gateway configuration to the FortiGate devices, in order for the interfaces to be displayed within Policy & Objects on FortiManager
B. Set up all of the phase 1 settings in the VPN community that they neglected to set up initiall
C. The interfaces will be automatically generated after the administrator configures all of the required settings.
D. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.
E. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

Answer: A

Explanation:
* - Create a VPN Community 2- Install VPN Configuration 3- Add IPsec Firewall Policies 4- Install the Policies

NEW QUESTION 34
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-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 39
A FortiGate has two default routes:

```
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

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

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre·dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

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

Answer: D

NEW QUESTION 44
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 47
Which statement is true regarding File description (FD) conserve mode?

A. IPS inspection is affected when FortiGate enters FD conserve mode.
B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
C. FD conserve mode affects all daemons running on the device.
D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 48
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.

Answer: B

Explanation:

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

NEW QUESTION 52
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. Only the DR receives link state information from non-DR routers.
B. Non-DR and non-BDR routers form full adjacencies to DR only.
C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C

Explanation:
Some special IP multicast addresses are reserved for OSPF: 224.0.0.5: All OSPF routers must be able to transmit and listen to this address. 224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

NEW QUESTION 54
An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.
What can the administrator do to fix this problem?

A. Configure remote link monitoring to detect an issue in the forwarding path.
B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
D. Configure set link-failed-signal enable under config system ha on both cluster members.

Answer: D

Explanation:
Virtual MAC Address and Failover - The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port. - Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces): #Config system ha set link-failed-signal enable end - This simulates a link failure that clears the related entries from MAC table of the switches.

NEW QUESTION 56
Refer to the exhibit, which shows the output of a web filtering diagnose command.

Which configuration change would result in non-zero results in the cache statistics section?

A. set server-type rating under config system central-management
B. set webfilter-cache enable under config system fortiguard
C. set webfilter-force-off disable under config system fortiguard
D. set ngfw-mode policy-based under config system settings

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 362

NEW QUESTION 59
Refer to the exhibit, which shows a partial routing table.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C       10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C       10.1.0.0/24 is directly connected, port3
S       10.10.4.0/24 [10/0] via 10.1.0.100, port3
C       10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S       10.1.0.0/24 [10/0] via 10.72.3.254, port4
C       10.72.3.0/24 is directly connected, port4
S       192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, what two changes would an administrator need to make if they wanted to send traffic from a client directly connected to port3, to a server directly connected to port4? (Choose two.)

A. Configure route leaking between VRF 12 and VRF 21.
B. Disable auto-asic-offload as this is not supported between VRF instances.
C. Configure RIPv2 to exchange route information between the VRF instances.
D. Configure route leaking between port3 and port4.
E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

Answer: AE

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148, 159

NEW QUESTION 63
Which two 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 devices.

Answer: AD

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins
There are 4 main wizards:Add Device: is used to add devices to central management and import their configurations.
Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.
Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

NEW QUESTION 64
Which two statements about conserve mode are true? (Choose two.)

A. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
B. FortiGate starts dropping all new sessions when the system memory reaches the configured redthreshold.
C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
D. FortiGate exits conserve mode when the system memory goes below the configured green threshold.

Answer: AD

NEW QUESTION 67
Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

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

Answer: B

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

NEW QUESTION 68
Examine the output from the 'diagnose debug authd fsso list' command; then answer the question below.
diagnose debug authd fsso list —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The
IP address 192.168.3.1 is
NOT the one used by the workstation INTERNAL2. TRAINING. LAB.
What should the administrator check?

A. The IP address recorded in the logon event for the user STUDENT.
B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
C. LAB.
D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
E. LAB.
F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 70
Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Installing configuration changes to managed devices
B. Importing interface mappings from managed devices
C. Adding devices to FortiManager
D. Previewing pending configuration changes for managed devices

Answer: AD

NEW QUESTION 73
Refer to the exhibit, which shows a partial routing table.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C        10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C        10.1.0.0/24 is directly connected, port3
S        10.10.4.0/24 [10/0] via 10.1.0.100, port3
C        10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S        10.1.0.0/24 [10/0] via 10.72.3.254, port4
C        10.72.3.0/24 is directly connected, port4
```

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

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

Answer: AB

NEW QUESTION 76
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server
name indication (SNI) extension?

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

Answer: A

NEW QUESTION 79
View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

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

Neighbor      V    AS    MsgRcvd   MsgSent  TblVer  InQ  OutQ  Up/Down   State/PfxRcd
10.125.0.60   4   65060   1698       1756     103    0    0   03:02:49      1
10.127.0.75   4   65075   2206       2250     102    0    0   02:45:55      1
10.200.3.1    4   65501    101        115       0    0    0   never       Active

Total number of neighbors 3
```

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

A. For the peer 10.125.0.60, the BGP state of is Established.
B. The local BGP peer has received a total of three BGP prefixes.
C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: AD

NEW QUESTION 81
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
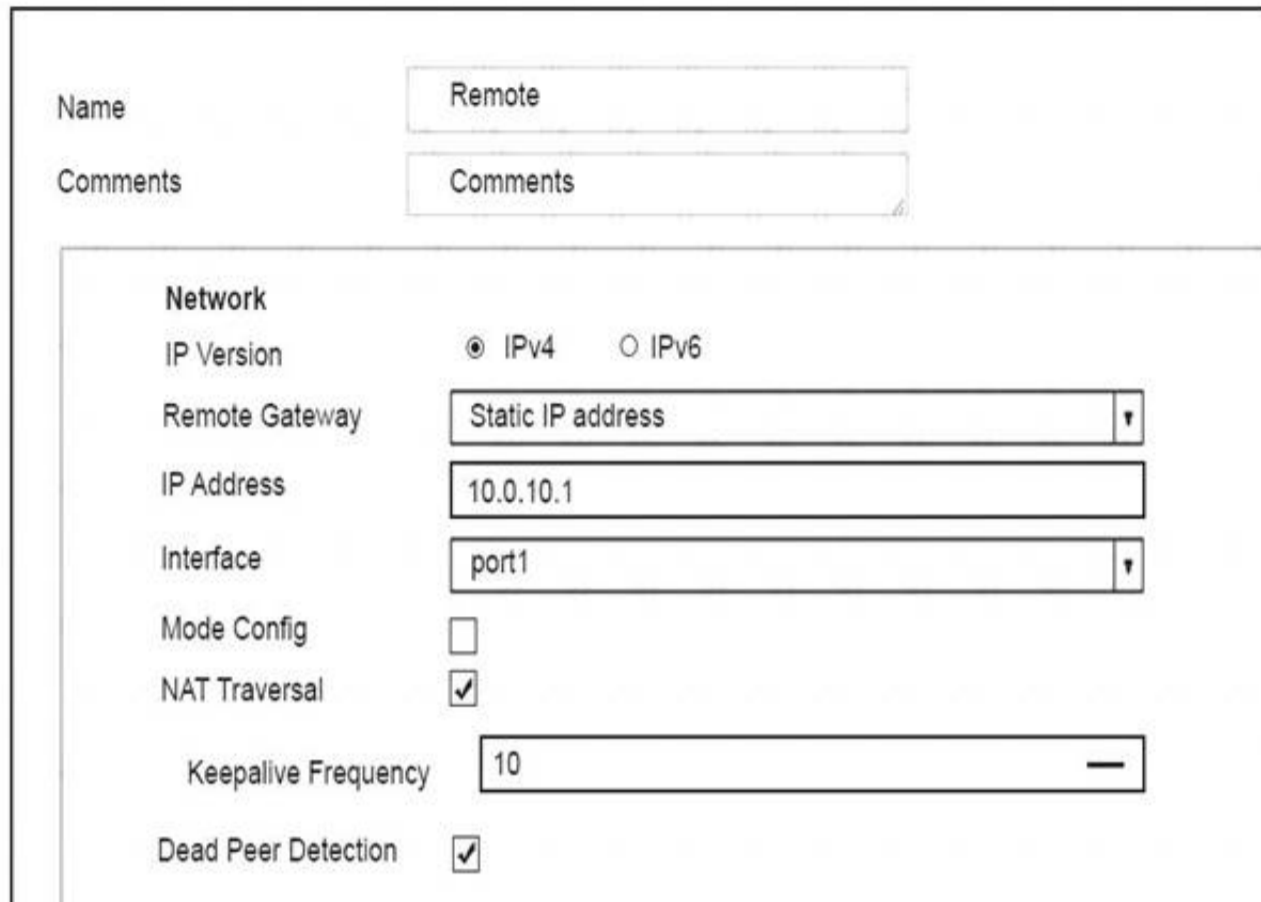
gateway to resolve the phase 1 negotiation error?

A. Change phase 1 encryption to 3DES and authentication to SHA128.
B. Change phase 1 encryption to AES128 and authentication to SHA512.
C. Change phase 1 encryption to AESCBC and authentication to SHA2.
D. Change phase 1 encryption to AES256 and authentication to SHA256.

Answer: D

NEW QUESTION 86
View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```
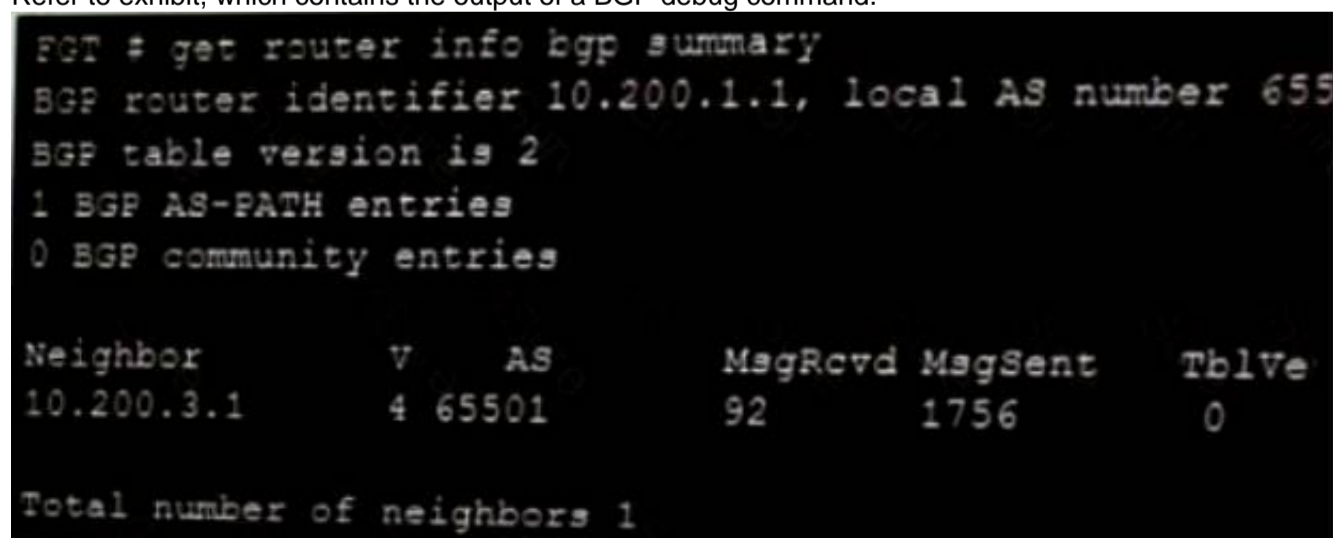
However, the IKE real time debug does not show any output. Why?

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

Answer: B

NEW QUESTION 87
Refer to exhibit, which contains the output of a BGP debug command.

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
B. The TCP session to 10.200.3.1 has not completed the three-way handshake.
C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.

D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:
BGP neighbor states and how they change:• Idle: Initial state• Connect: Waiting for a successful three-way TCP connection• Active: Unable to establish the TCP session• OpenSent: Waiting for an OPEN message from the peer• OpenConfirm: Waiting for the keepalive message from the peer• Established: Peers have successfully exchanged OPEN and keepalive messages

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

```
# diagnose webfilter fortiguard statistics list          # diagnose webfilter fortiguard statistics list

Raring Statistics:                                        Cache Statistics:
===========================                               =======================

DNS filures             :      273                        Maximum memory      :      0
DNS lookups             :      280                        Memory usage        :      0
Data send failures      :        0
Data read failures      :        0                        Nodes               :      0
Wrong package type      :        0                          Leaves            :      0
Hash table miss         :        0                          Prefix nodes      :      0
Unknown server          :        0                          Exact nodes       :      0
Incorrect CRC           :        0
Proxy requests failures :        0                        Requests            :      0
Request timeout         :        1                        Misses              :      0
Total requests          :     2409                        Hits                :      0
Requests to FortiGuard servers :  1182                      Prefix hits       :      0
Server errored responses :       0                          Exact hits        :      0
Relayed rating          :        0
Invalid profile         :        0                        No cache directives :      0
                                                          Add after prefix    :      0
Allowed                 :     1021                        Invalid DB put      :      0
Blocked                 :     3909                        DB updates          :      0
Logged                  :     3927
Blocked Errors          :      565                        Percent full        :     0%
Allowed Errors          :        0                          Branches          :     0%
Monitors                :        0                          Leaves            :     0%
Authenticates           :        0                            Prefix nodes    :     0%
Warnings                :       18                            Exact nodes     :     0%
Ovrd request timeout    :        0
Ovrd send failures      :        0                        Miss rate           :     0%
Ovrd read failures      :        0                        Hit rate            :     0%
Ovrd errored responses  :        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.

Answer: C

NEW QUESTION 93
Refer to the exhibits.

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

Which contain the partial configurations of two VPNs on FortiGate.

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must administrator make to fix the issue? (Choose two.)

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

Answer: CD

Explanation:
To set peer-id, the VPN must be set in aggressive mode - https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-Peer-IDs-to-select-an-IPSec-dialup/ta-p

NEW QUESTION 94
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
iike 0:620000:98:           type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

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

A. In the phase 1 network configuration, set the IKE version to 2.
B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.
C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

Answer: D

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852

NEW QUESTION 96
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
B. Only the root FortiGate sends logs to FortiAnalyzer.
C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

Answer: AC

Explanation:
FortiGate's to Root uses FortiTelemetry (TCP-8013) FortiTelemetry is also used for FortiClient communication Root Fortigate to FortiAnalyzer uses API (TCP-443)

NEW QUESTION 98
Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

```
Configuration  Session

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
```

```
Configuration  Session

FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
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)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
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
no_ofld_reason:
```

An administrator would like to test session failover between the two service provider connections.
What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Configure set snat-route-change enable.
B. Change the priority of the port2 static route to 5.
C. Change the priority of the port1 static route to 11.
D. unset snat-route-change to return it to the default setting.

Answer: AC

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148-149

NEW QUESTION 103
Refer to the exhibit, which contains the output of the diagnose vpn tunnel list. Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any 'esp and host 10.200.3.2'
B. diagnose sniffer packet any 'ip proto 50'
C. diagnose sniffer packet any 'host 10.0.10.10'
D. diagnose sniffer packet any 'port 4500'

Answer: D

NEW QUESTION 106
What is the purpose of an internal segmentation firewall (ISFW)?

A. It inspects incoming traffic to protect services in the corporate DMZ.
B. It is the first line of defense at the network perimeter.
C. It splits the network into multiple security segments to minimize the impact of breaches.
D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

Answer: C

Explanation:
ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

NEW QUESTION 107
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254

...

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

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

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

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc

...

ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

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

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

Answer: B

NEW QUESTION 111
Refer to the exhibit, which shows partial outputs from two routing debug commands.

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

Routing table for VRF=0
S        0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S    *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

Routing table for VRF=0
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 output?

A. The port2 interface is disabled in the FortiGate configuration.
B. The port1 default route has a lower distance than the default route using port2.
C. The port1 default route has a higher priority value than the default route using port2.
D. The port1 default route has a lower priority value than the default route using port2.

Answer: B

NEW QUESTION 114
Refer to the exhibit, which contains the output of a debug command.

```
# 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
```

If the default settings are in place, what can be concluded about the conserve mode shown in the exhibit?

A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.
B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Answer: C

NEW QUESTION 116
Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # 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
100.64.3.1      4 65501    101     115     0       0   0   never        Active

Total number of neighbors 3
```

What can be concluded about the router in this scenario?

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the BGP session with the local router.
B. The State/PfxRcd for neighbor 100.64.3.1 will not change until an administrator on the local router adjusts the inbound route filtering so that prefixes received can be added to the RIB.
C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
D. The BGP session with peer 10.127.0.75 is up.

Answer: D

NEW QUESTION 121
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 125
Refer to the exhibit, which shows the output of a diagnose command.

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon 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
```

What can be concluded about the debug output in this scenario?

A. Servers with a negative TZ value are less preferred for rating requests.
B. There is a natural correlation between the value in the Packets field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

Answer: B

NEW QUESTION 128
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

Answer: B

NEW QUESTION 133
View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

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

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which of the following statements is true regarding this output?

A. The requested URL belongs to category ID 255.
B. The server hostname Is training, fortinet.com.
C. FortiGate found the requested URL in its local cache.
D. This web request was inspected using the ftgd-allow web filler profile.

Answer: C

Explanation:
Example log for no local cache case: #id=93000 msg="pid=57 urlfilter_main-723 in main.c received pkt:count=91 "IPS and WAD will only send request to urlfilter daemon when cache is missed. " So the WAD process by itself found the URL rating in the local cache and didn`t ask for help from the URL process as in the example.

NEW QUESTION 137
Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

```
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
```

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
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)
src_mac=b4:f7a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
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=0x0000/0x000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

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

Answer: D

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-SNAT-route-change-to-update-existing-NAT/

NEW QUESTION 139
An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

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

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

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

A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
B. Redirection of HTTP to HTTPS administrative access is disabled.
C. HTTP administrative access is configured with a port number different than 80.

D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 144
......

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-7.0 Practice Exam Features:

* NSE7_EFW-7.0 Questions and Answers Updated Frequently

* NSE7_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-7.0 Practice Test Here](https://www.certshared.com/exam/NSE7_EFW-7.0/)