Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
Which two statements about bulk configuration changes made using FortiManager CLI scripts are correct? (Choose two.)

A. When run on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate device.
B. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
C. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.
D. When run on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate device.

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
Refer to the exhibit, which shows a session table entry.

Which statement about FortiGate behavior relating to this session is true?

A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
B. FortiGate forwarded this session without any inspection.
C. FortiGate is performing security profile inspection using the CP
D. FortiGate applied only IPS inspection to this session.

Answer: C

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 91, 92 First digit of "proto_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage

NEW QUESTION 4
Refer to the exhibit, which shows 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 device is 0, what will happen if the primary fails and the secondary becomes the primary?

A. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.
B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.
C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.
D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-see-if-a-session-is-synced-in-HA/ta-p/1941

NEW QUESTION 5
Refer to the exhibit, which contains 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
```
Which statement about the exhibit is true?

A. The local router has received a total of three BGP prefixes from all peers.
B. The local router has not established a TCP session with 100.64.3.1.
C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

NEW QUESTION 6
The CLI command set intelligent-mode <enable | disable> controls the IPS engine's adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

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

Answer: C

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

NEW QUESTION 7
Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected

as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

A. 1
B. 2
C. 3
D. 4

Answer: B

NEW QUESTION 8
How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

A. FortiManager can download and maintain local copies of FortiGuard databases.
B. FortiManager supports only FortiGuard push to managed devices.
C. FortiManager will respond to update requests only if they originate from a managed device.
D. FortiManager does not support rating requests.

Answer: A

NEW QUESTION 9
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 10
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
BAF47D0988E9237F2F405EF3952F6FDA011004000000000000001AE0400003C0000000100000001000000300101000
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD AFCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:     protocol id - ISAKMP:
ike 0: RemoteSite:4:          trans_id - KEY_IKE.
ike 0: RemoteSite:4:          encapsulation - IKE/none
ike 0: RemoteSite:4:              type=OAKLEY_ENCRYPT_ALG,  val=AES_CBC, key-len=128
ike 0: RemoteSite:4:              type=OAKLEY_HASH_ALG, val=SHA
ike 0: RemoteSite:4:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:              type=OAKLEY_GROUP, val=MODF1024.
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
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000080140000181F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```
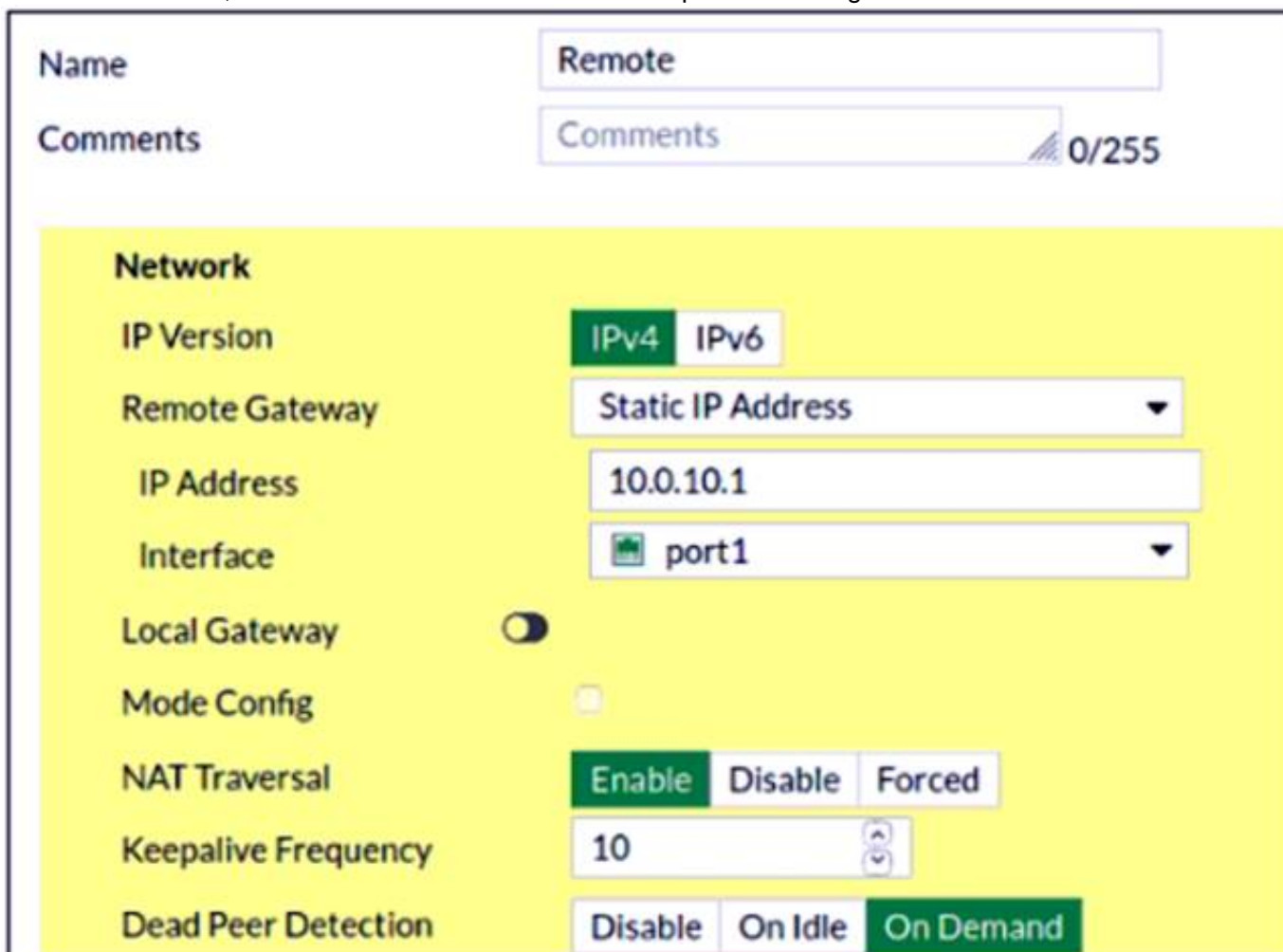
Which statements about this debug output are correct? (Choose two.)

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

Answer: BD

NEW QUESTION 10
Refer to the exhibit, which contains a screenshot of some phase 1 settings.

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1
However, the IKE real-time debug does not show any output. Why?

A. The administrator must also run the command diagnose debug enable.
B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.
C. The log-filter setting is incorrec
D. The VPN traffic does not match this filter.
E. The debug shows only error message
F. If there is no output, then the phase 1 and phase 2 configurations match.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPSec-VPN-Diagnostics-Possible-reasons/ta-p/1920

NEW QUESTION 11
View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.

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

Answer: B

Explanation:
fortigate does it in order Static URL -> FortiGuard – > Content -> Advanced (java, cookie removal..)so block it in first step

NEW QUESTION 16
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
      name: 'Hub2Spoke1'
      auto-negotiate: disable
      mode: tunnel
      src: 0:192.168.1.0/0.0.0.0:0
      dst: 0:10.10.20.0/0.0.0.0:0
      SA
        lifetime/rekey: 43200/32137
        mtu: 1438
        tx-esp-seq: 2ce
        replay: enabled
        inbound
          spi: 01e54b14
          enc:  aes-cb 914dc5d092667ed436ea7f6efb867976
          auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
        outbound
          spi: 3dd3545f
          enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
```

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

A. Phase 2 authentication is set to sha1 on both sides.
B. Anti-replay is disabled.
C. Hub2Spoke1 is a policy-based VPN.
D. Hub2Spoke1 is configured on interface wan2.

Answer: AD

NEW QUESTION 20
Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.

```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session    ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_dst_session   ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_scan          ip=192.168.1.110   dos_id=1  exp=649   pps=0  freq=0
id=udp_flood         ip=192.168.1.110   dos_id=2  exp=653   pps=0  freq=0
id=tcp_src_session   ip=192.168.1.110   dos_id=1  exp=5175  pps=0  freq=8
id=tcp_port_scan     ip=192.168.1.110   dos_id=1  exp=175   pps=0  freq=0
id=ip_src_session    ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=30
id=udp_src_session   ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.
B. Those whose traffic matches an IPS sensor.
C. Those whose traffic exceeded a threshold of a matching DoS policy.
D. Those whose traffic was detected as an anomaly by an IPS sensor.

Answer: A

NEW QUESTION 22
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:253000:27: responder: main mode get 1st message...
ike 0:253000:27: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:253000:27: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:253000:27: incoming proposal:
ike 0:253000:27: proposal id = 0:
ike 0:253000:27:    protocol id = ISAKMP:
ike 0:253000:27:        trans_id = KEY_IKE.
ike 0:253000:27:        encapsulation = IKE/none
ike 0:253000:27:            type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:253000:27:            type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:253000:27:            type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:            type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: my proposal, gw Remotesite:
ike 0:253000:27: proposal id = 1:
ike 0:253000:27:    protocol id = ISAKMP:
ike 0:253000:27:        trans_id = KEY_IKE.
ike 0:253000:27:        encapsulation = IKE/none
ike 0:253000:27:            type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:253000:27:            type=OAKLEY_HASH_ALG, val=SHA.
ike 0:253000:27:            type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:            type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: negotiation failure
ike Negot:253a8cbe6335e6fd/0000000000000000:27: no SA proposal chosen
```

Why did the tunnel not come up?

A. The local gateway has configured less secure encryption and hashing algorithms compared to the remote gateway.
B. The Diffie-Hellman group does not match on the local and remote gateways.
C. The proposal ID does not match between local and remote gateways.
D. The encapsulation method for phase 2 is set to none on local and remote gateways.

Answer: A

Explanation:
local gateway: encryption AES-128, hash SHA remote gateway: encryption AES-256, hash SHA-256 So local gateway has less secure settings

NEW QUESTION 27
Which two statements about OCVPN are true? (Choose two.)

A. Only root vdom supports OCVPN.
B. OCVPN supports static and dynamic IPs in WAN interface.
C. OCVPN offers only Hub-Spoke VPNs.
D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: AB

NEW QUESTION 28
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 33
What is the diagnose test application ipsmenitor 5 command used for?

A. To enable IPS bypass mode
B. To disable the IPS engine
C. To restart all IPS engines and monitors
D. To provide information regarding IPS sessions

Answer: A

Explanation:
diagnose test application ipsmonitor 5: Toggle bypass status
* 13: IPS session list
* 98: Stop all IPS engines
* 99: Restart all IPS engines and monitor

NEW QUESTION 34
Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

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

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

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

Answer: AC

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

NEW QUESTION 38
View the global IPS configuration, and then answer the question below.

```
config ips global
    set fail-open disable
    set intelligent-mode disable
    set engine-count 0
    set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.
B. FortiGate will spawn IPS engine instances based on the system load.
C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.

D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Answer: A

NEW QUESTION 41
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 44
Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tup
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

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

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/1969

NEW QUESTION 46
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

```
# diagnose debug rating
Locale        : english
License       : Contract
Expiration    : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP                  Weight    RTT    Flags   TZ   Packets   Curr Lost   Total Los
69.195.205.101      10        45             -5   262432    0           846
69.195.205.102      10        46             -5   329072    0           6806
209.222.147.43      10        75             -5   71638     0           275
96.45.33.65         20        71             -8   36875     0           92
208.91.112.196      20        103    DI      -8   34784     0           1070
208.91.112.198      20        107    D       -8   35170     0           1533
80.85.69.41         60        144            0    33728     0           120
62.209.40.73        71        226            1    33797     0           192
121.111.236.180     150       197            9    33754     0           145
69.195.205.103      45        44     F       -5   26410     26226       26227
```

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

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
C. FortiGate will send the FortiGuard queries to the server with highest weight.
D. A server's round trip delay (RTT) is not used to calculate its weight.

Answer: BC

NEW QUESTION 51
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.

Answer: B

NEW QUESTION 52
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 55
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:    protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:    protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn't the tunnel come up?

A. The pre-shared keys do not match.
B. The remote gateway's phase 2 configuration does not match the local gateway's phase 2 configuration.
C. The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration.
D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Answer: C

NEW QUESTION 59
View the exhibit, which contains a partial routing table, and then answer the question below.

```
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, which of the following pings will FortiGate route? (Choose two.)

A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 61
Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

A. Primary unit stops sending HA heartbeat keepalives.
B. The FortiGuard license for the primary unit is updated.
C. One of the monitored interfaces in the primary unit is disconnected.
D. A secondary unit is removed from the HA cluster.

Answer: AC

NEW QUESTION 63
Which statement about IKE and IKE NAT-T is true?

A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.
B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.
C. They both use UDP as their transport protocol and the port number is configurable.
D. They each use their own IP protocol number.

Answer: C

Explanation:
IKE without NAT-T runs over UDP port 500. IKE with NAT-T runs over UDP port 4500. It can be configurable - https://docs.fortinet.com/document/fortigate/7.0.0/new-features/33578/configurable-ike-port

NEW QUESTION 65
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. FortiGate first checks the OSPF ID to elect a DR.
B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
C. BDR is responsible for forwarding link state information from one router to another.
D. Only the DR receives link state information from non-DR routers.

Answer: B

NEW QUESTION 67
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 72
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 76
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 80
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 81
What does the dirty flag mean in a FortiGate session configured for NGFW policy mode?

A. The existing session table entry has been updated with the app_id and the firewall policy table needs to be checked for a match.
B. The application or URL category is unknown and needs to be rescanned by the IPS engine to try to identify the Layer 7 details.
C. The URL category for this session has been updated by FortiGuard and the session needs to be checked against the policy again to ensure proper web filtering is applied.
D. Traffic has been identified as coming from an application that is not allowed and the relevant replacement message needs to be displayed to the user, if configured.

Answer: A

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 99

NEW QUESTION 86
What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

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

Answer: AD

NEW QUESTION 88
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 91
Refer to the exhibit, which contains a TCL script configuration on FortiManager.

Type	TCL Script ▼
Run script on	Remote FortiGate ... ▼
| Script details | ```
#!
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# " 10]
}
run_cmd "config system interface "
run_cmd "edit port1"
run_cmd "set ip 10.0.1.10 255.255.255.0"
run_cmd "next"
run_cmd "end"
``` |

An administrator has configured the TCL script on FortiManager, but failed to apply any changes to the managed device after being executed.
Why did the TCL script fail to make any changes to the managed device?

A. Changes in an interface configuration can only be done by CLI script.
B. The TCL script must start with #include <>.
C. Incomplete commands are ignored in TCL scripts.
D. The TCL command run_cmd has not been created.

Answer: D

NEW QUESTION 96
View the exhibit, which contains the output of a debug command, and then answer the question below.

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

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

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

Answer: BC

NEW QUESTION 101
The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

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

Answer: C

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

NEW QUESTION 102
View the exhibit, which contains the partial output of a diagnose command, and then answer the question below.

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

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

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

Answer: A

NEW QUESTION 106
Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. set av-failopen off

B. set av-failopen pass
C. set fail-open enable
D. set ips fail-open disable

Answer: AC

Explanation:
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserve-mode

NEW QUESTION 111
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:9268ab9dea63aa3/00000000000000000:591: responder: main mode get 1st message…
...
ike 0:9268ab9dea63aa3/00000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/00000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/00000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:       trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/00000000000000000:591:       encapsulation = IKE/none
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/00000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/00000000000000000:591: proposal id=0:
ike 0:9268ab9dea63aa3/00000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:       trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/00000000000000000:591:       encapsulation = IKE/none
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/00000000000000000:591:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/00000000000000000:591: ISA KMP SA lifetime=86400
ike 0:9268ab9dea63aa3/00000000000000000:591: my proposal, gw VPN:
ike 0:9268ab9dea63aa3/00000000000000000:591:     proposal id = 1:
ike 0:9268ab9dea63aa3/00000000000000000:591:       protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:         trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/00000000000000000:591:         encapsulation = IKE/none
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/00000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/00000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/00000000000000000:591:       protocol_id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:         trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/00000000000000000:591:         encapsulation = IKE/none
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/00000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/00000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/00000000000000000:591:       protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:         trans_id = ISAKMP:
ike 0:9268ab9dea63aa3/00000000000000000:591:         encapsulation = IKE/none
ike 0:9268ab9dea63aa3/00000000000000000:591:            type= OAKLEY_ENCRYPT_ALG, val =AES-CBC,
key-len=128
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/00000000000000000:591:            type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/00000000000000000:591: 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 115
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 120
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 122
Refer to the exhibit, which shows the output of a diagnose command.

```
# diagnose sys session list expectation

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

What can you conclude from the output shown in the exhibit? (Choose two.)

A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.
B. This is an expected session created by the IPS engine.
C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.
D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to thenext-hop IP address 10.0.1.10.

Answer: AD

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 110, 111, 115

NEW QUESTION 125
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
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
...		

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
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.

Answer: C

NEW QUESTION 127
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 130
An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

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

Answer: A

NEW QUESTION 133
Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State        Dead Time   Address        Interface
0.0.0.69        1     Full/DR      00:00:32    10.126.0.69    wan1
0.0.0.117       1     Full/DROther 00:00:34    10.126.0.117   wan2
0.0.0.2         1     Full/ -      00:00:38    172.16.1.2     ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.
B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.
C. There are more than two OSPF routers on the wan2 network.
D. The interface ToRemote is a broadcast OSPF network.

Answer: C

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

NEW QUESTION 136

What is the diagnose test application ipsmonitor 99 command used for?

A. To enable IPS bypass mode
B. To provide information regarding IPS sessions
C. To disable the IPS engine
D. To restart all IPS engines and monitors

Answer: D

NEW QUESTION 139
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
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)
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 143
In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

A. It provides VM license validation services.
B. It supports rating requests from non-FortiGate devices.
C. It caches available firmware updates for unmanaged devices.
D. It can be configured as an update server, a rating server, or both.

Answer: AD

NEW QUESTION 144
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 149
Refer to the exhibit, which contains partial outputs from two routing debug commands.

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

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

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

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

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

Answer: D

NEW QUESTION 152
An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

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

Answer: BC

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

NEW QUESTION 153
An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMSs in FortiManager.
How should the administrator accomplish this task?

A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.
B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.
C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.
D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 244

NEW QUESTION 154
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 157
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 161
An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

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

Answer: BDE

NEW QUESTION 164
Refer to the exhibit, which shows the output of diagnose sys session stat.

```
NGFW-1 # diagnose sys session stat
misc info:         session_count=591 setup_rate=0 exp_count=0 clash=162
         memory_tension_drop=0 ephemeral=0/65536 removeable=0
delete=0, flush=0, dev_down=0/0 ses_walkers=0
TCP sessions:
         166 in NONE state
         1 in ESTABLISHED state
         3 in SYN_SENT state
         2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

Which statement about the output shown in the exhibit is correct?

A. There are two sessions that have not been removed in case of any out-of-order packets that arrive.
B. There are 166 TCP sessions waiting to complete the three-way handshake.
C. 162 sessions have been deleted because of memory page exhaustion.
D. All the sessions in the session table are TCP sessions.

Answer: A

NEW QUESTION 167
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 169
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 170
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 174
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 179
Which two tasks are automated using the Import Configuration wizard on FortiManager? (Choose two.)

A. Importing firewall address objects from managed devices
B. Importing interface mappings from managed devices
C. Importing static and dynamic route configurations from managed devices
D. Importing devices to FortiManager

Answer: AB

Explanation:
https://docs.fortinet.com/document/fortimanager/7.0.5/administration-guide/337348

NEW QUESTION 184
Which of the following statements are correct regarding application layer test commands? (Choose two.)

A. They are used to filter real-time debugs.
B. They display real-time application debugs.
C. Some of them display statistics and configuration information about a feature or process.
D. Some of them can be used to restart an application.

Answer: CD

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

NEW QUESTION 186
What does the dirty flag mean in a FortiGate session?

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

Answer: B

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

NEW QUESTION 191

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
qwy=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.

Answer: D

NEW QUESTION 194

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 199
......

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.surepassexam.com/NSE7_EFW-7.0-exam-dumps.html)