NSE7_EFW-6.2.VCEplus.premium.exam.30q

Number: NSE7_EFW-6.2
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

NSE7_EFW-6.2

Fortinet NSE 7 - Enterprise Firewall 6.2

Version 1.0

Exam A

QUESTION 1 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`

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Refer to the exhibit, which contains the partial output of a diagnose command.

```
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=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqmo=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
     src: 0:10.1.2.0/255.255.255.0:0
     dat: 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=204B seqno=1
esn=replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
          ah=sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

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

A. Anti-replay is enabled.
B. DPD is disabled.
C. Remote gateway IP is 10.200.4.1.
D. Quick mode selectors are disabled.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Refer to the exhibit, which contains 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
```

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

A. FortiGate will probe `121.111.236.179` every fifteen minutes for a response.
B. Servers with a negative `TZ` value are experiencing a service outage.
C. Servers with the `D` flag are considered to be down.
D. FortiGate used `209.222.147.36` as the initial server to validate its contract.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 Which two statements about application layer test commands are true?
(Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Refer to the exhibits, which contain configuration on FortiGate and partial session information.

```
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
```

```
PGT # 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:
```

All traffic to the Internet currently egresses from `port1`. The exhibit shows partial session information for Internet traffic from a user on the internal network.

If the priority on route ID 1 were changed from `5` to `20`, what would happen to traffic matching that user's session?

A. The session would remain in the session table, but its traffic would now egress from both `port1` and `port2`.
B. The session would remain in the session table, and its traffic would still egress from `port1`.

C. The session would remain in the session table, and its traffic would start to egress from `port2`.
D. The session would be deleted, so the client would need to start a new session.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6 Which three conditions are required for two FortiGate devices to form an OSP adjacency? (Choose three.)

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

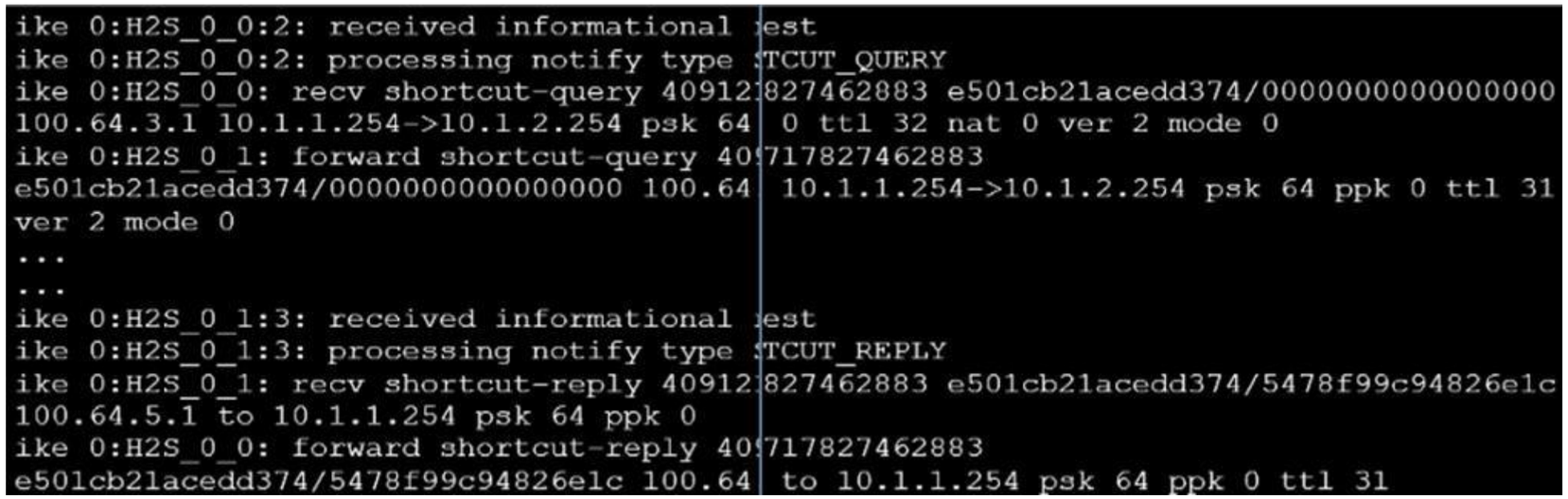
QUESTION 7 Which two statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Refer to the exhibit, which contains a partial output of an IKE real-time debug.



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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Refer to the exhibit, which contains a session table entry.

```
FGI # diagnose sys session  list
session info: proto=6 proto_state-11 duration-35 expire-265  timeout=300 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-redir local may_dirty none app_ntf
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=7->6/ 6->7 gwy=172.20.12.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:4954->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545
(192.167.1.100:49545)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac-08:5b:0e:6c:7b:7a
misc=0 policy_id-21 auth_info=0 chk_client_info=0 vd=0
serial-007f2948 tos-ff/ff app_list=0 app-0 url_cat-41
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=
0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

Which statement about FortiGate inspection of this session is true?

A. FortiGate applied proxy-based inspection.
B. FortiGate applied flow-based NGFW policy-based inspection.
C. FortiGate applied flow-based inspection.
D. FortiGate forwarded this session without any inspection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Refer to the exhibit, which contains the output of a debug command.

```
FGT # 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 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

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

A. The local FortiGate OSPF router ID is `0.0.0.4`.
B. The local FortiGate is the backup designated router.
C. In the network connected to `port4`, two OSPF routers are down.
D. `Port4` is connected to the OSPF backbone area.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Refer to the exhibit, which contains the output of `diagnose sys session stat`.

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

Which two statements about the output shown are correct? (Choose two.)

A. No sessions have been deleted because of memory pages exhaustion.
B. There are 0 ephemeral sessions.
C. There are 168 TCP sessions waiting to complete the three-way handshake.
D. All the sessions in the session table are TCP sessions.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Refer to the exhibit, which contains central management configuration.

```
config system central-management
    set type fortimanager
    set fmg "10.0.1.242"
    config server-list
        edit 1
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.240
        next
        edit 2
            set server-type update
            set addr-type ipv4
            set server-address 10.0.1.243
        next
        edit 3
            set server-type rating
            set addr-type ipv4
            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. `10.0.1.242`
B. `10.0.1.244`
C. Public FortiGuard servers
D. `10.0.1.240`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Refer to the exhibit, which contains the partial output of an IKE real-time debug.

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder
message…
…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id=0:
ike 0:c49e59846861b0f6/0000000000000000:278:      protocol id = IMAKMP:
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 ike 0:c49e59846861b0f6/0000000000000000:278: no SA
proposal chosen
```

Why did the tunnel *not* come up?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator notices 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 about this command is true?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 What does the `dirty` flag mean in a
FortiGate session?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Refer to the exhibit, which contains 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

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 outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. port3
B. port2
C. port1
D. Both port1 and port2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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
```

Which statement about this FortiGate is correct?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 How does FortiManager handle FortiGate requests from FortiGate devices, when it is configured as a local FDS?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Refer to the exhibit, which contains the output of a web filtering diagnose command.

```
# diagnose webfilter fortiguard statistics list # diagnose webfilter fortiguard statistics list
...
Rating Statistics:                          Cache Statistics:
==================                          =================
DNS failures                 :    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 request 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 chache 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 statement explains why the cache statistics are all zeros?

A. The FortiGate web filter cache is disabled in the FortiGate configuration.
B. FortiGate is using flow-based inspection which does not use the cache.
C. The administrator has reallocated the cache memory to a separate process.
D. There are no users making web requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
An administrator wants to capture ESP 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 execute?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24 Which two conditions must be met for a statistic route to be active in the routing table?
(Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Refer to the exhibit, which contains the output of a real-time debug.

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

msg= "received a request /tmp/ .ipsengine_176_0_0.url.socket, addr_len=37:
d=training.fortinet.com:80, id=289, cat=255, vfname= 'root', vfid=0, profile= 'default',
type=0, client=10.0.1.10, url_source=1, url= "/"
msg= "Cache miss" user= "N/A" src=10.0.1.10 sport=54218 dst=13.33.165.116 dport=80
service= "http" hostname = "training.fortinet.com" url= "/" action=9 (ftgd-block) wf-
act=3 (BLOCK) user= "N/A" src=10.0.1.10 sport=54218 dst=13.33.165.116 dport=80
service= "http"cat=52 hostname= "training fortinet.com" url= "/"
```

Which statement regarding this output is true?

A. FortiGate found the requested URL in its local cache.
B. The requested URL belongs to category ID 52.
C. The client hostname is `training.fortinet.com`.
D. This web request was inspected using the `root` web filter profile.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 Which two tasks are automated using the **Install Wizard** on FortiManager? (Choose two.)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Refer to the exhibit, which contains 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
...
```

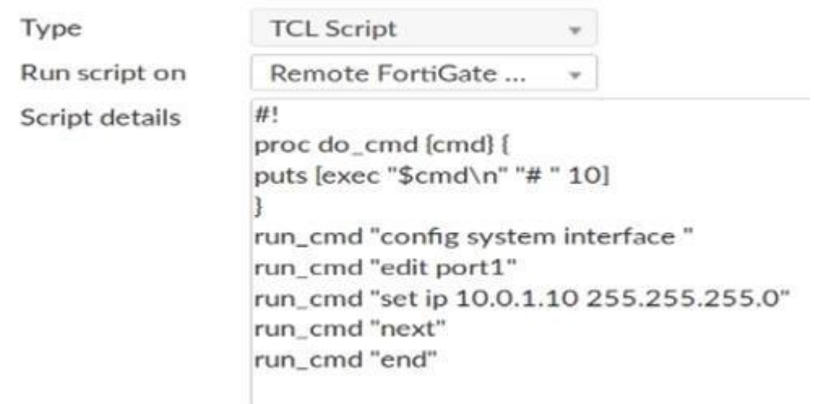
Assuming all the appropriate firewall policies are configured, which two pings will FortiGate route? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Refer to the exhibit, which contains a TCL script configuration on FortiManager.



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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Refer to the exhibit, which contains the partial output of an IKE real-time debug.

```
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
BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C000000010000000100000030010100O
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
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000000801400001 81F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA0810040100000000000000 8c2E3FC9BA061816A396F009A12
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 two statements about this debug output are correct? (Choose two.)

A. The initiator has provided `remote` as its IPsec peer ID.
B. The negotiation is using AES128 encryption with CBC hash.

C. The remote gateway IP address is 10.0.0.1.
D. It shows a phase 1 negotiation.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference: