Number: NSE7
Passing Score: 800
Time Limit: 120 min
File Version: 4.1

VCEplus
VCE To PDF - Free Practice Exam

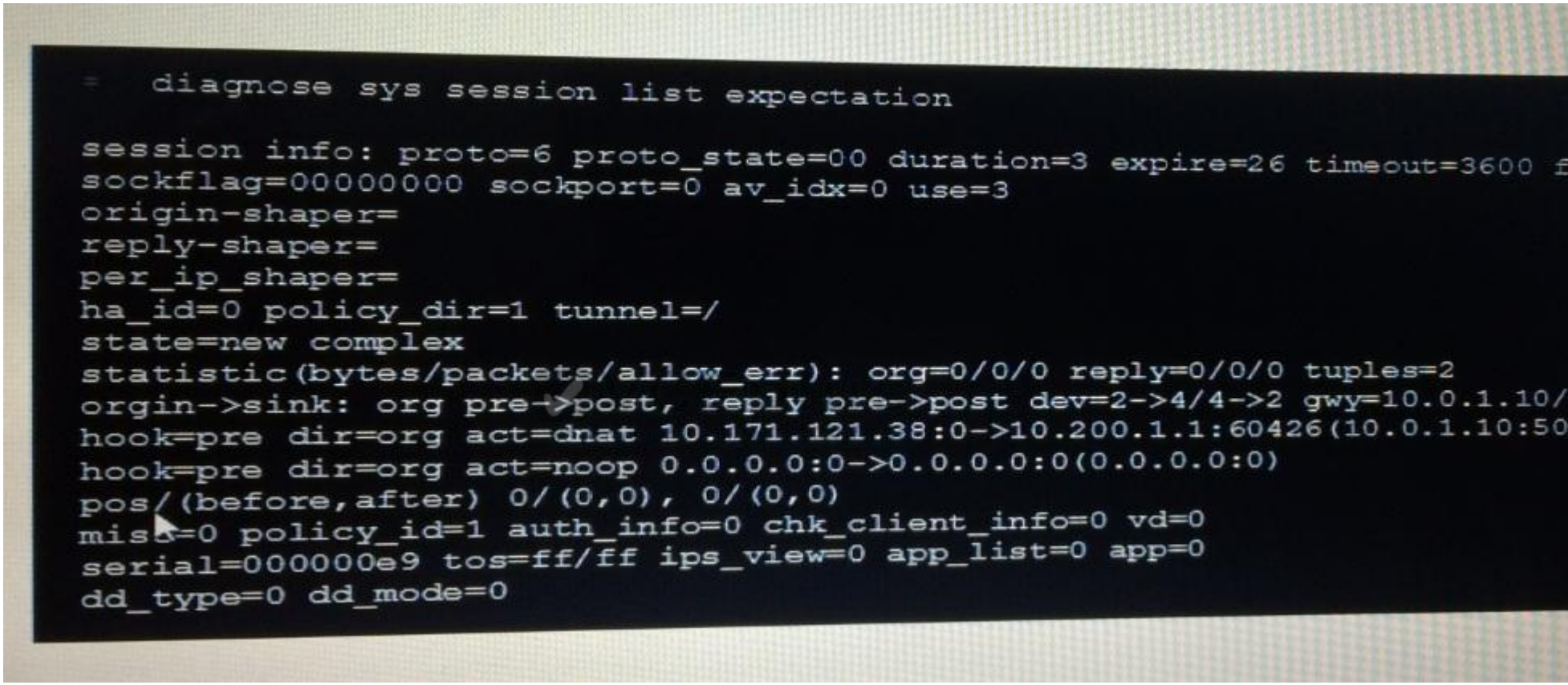
NSE7

Fortinet Troubleshooting Professional

VCEplus
VCE To PDF - Free Practice Exam

Exam A

QUESTION 1
Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; then answer the question below.



Which statement is true regarding the session in the exhibit?

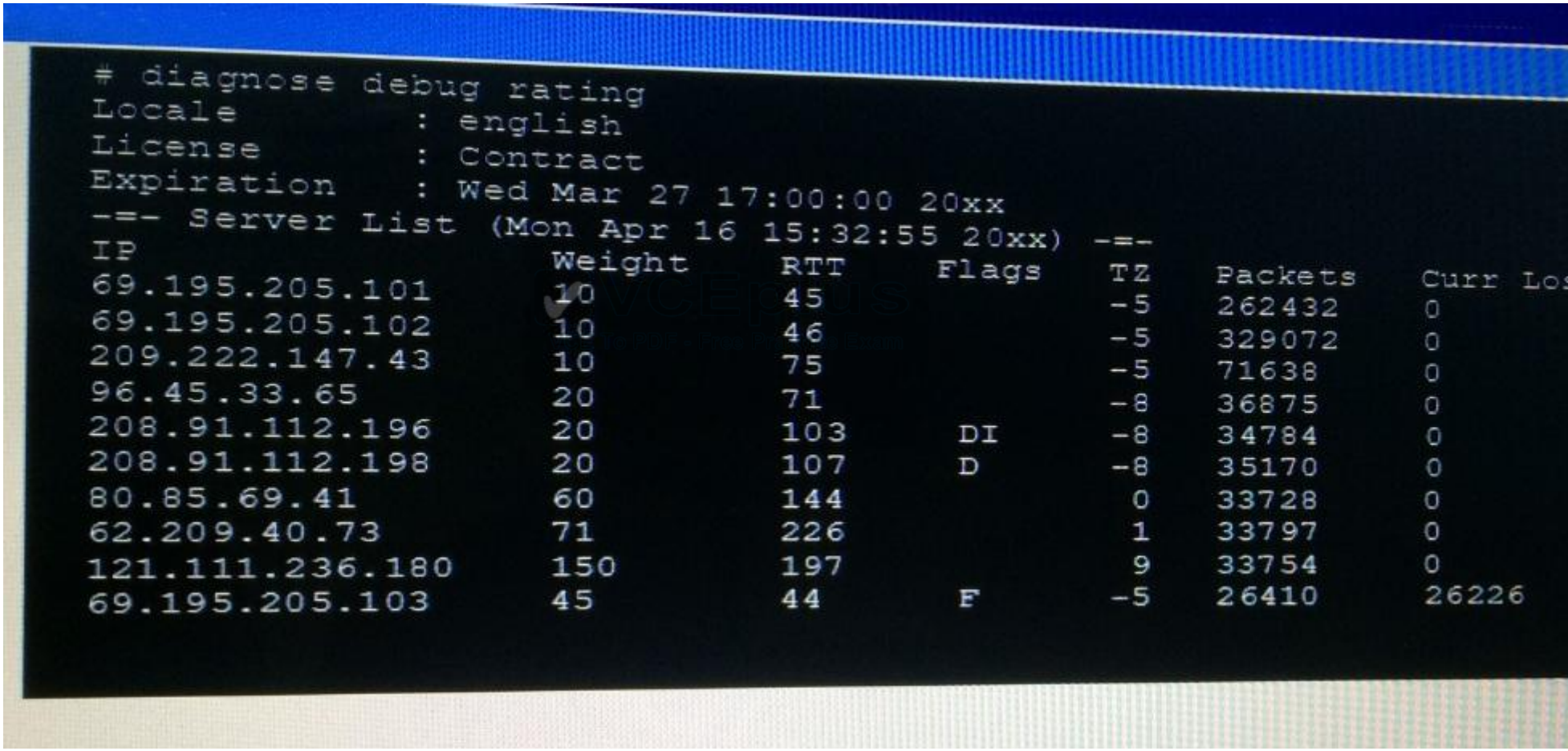
A. It was created by the FortiGate kernel to allow push updates from FortiGuard.
B. It is for management traffic terminating at the FortiGate.
C. It is for traffic originated from the FortiGate.
D. It was created by a session helper or ALG.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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 Lo
69.195.205.101       10        45             -5    262432     0
69.195.205.102       10        46             -5    329072     0
209.222.147.43       10        75             -5    71638      0
96.45.33.65          20        71             -8    36875      0
208.91.112.196       20        103     DI     -8    34784      0
208.91.112.198       20        107     D      -8    35170      0
80.85.69.41          60        144             0    33728      0
62.209.40.73         71        226             1    33797      0
121.111.236.180      150       197             9    33754      0
69.195.205.103       45        44      F      -5    26410      26226
```

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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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. TRAINING. LAB.
C. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING. LAB.
D. The reserve DNS lookup for the IP address 192.168.3.1.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A FortiGate's port1 is connected to a private network. Its `port2` is connected to the Internet. Explicit web proxy is enabled in `port1` and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the `local` flag on.
B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.

C. One session has the `proxy` flag on, the other one does not.
D. One of the sessions has the IP address of port2 as the source IP address.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
When does a RADIUS server send an *Access-Challenge* packet?

A. The server does not have the user credentials yet.
B. The server requires more information from the user, such as the token code for two-factor authentication.
C. The user credentials are wrong.
D. The user account is not found in the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

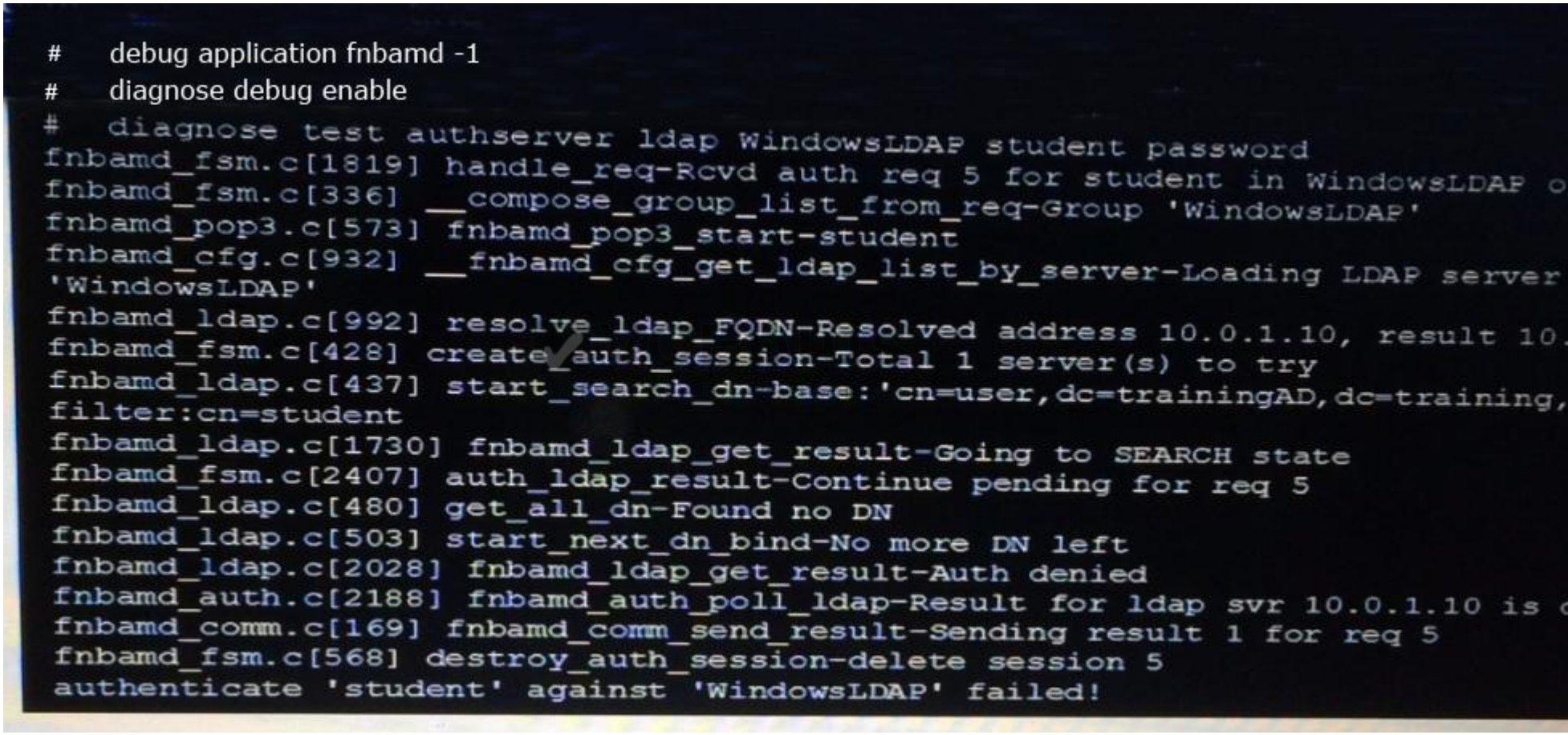
QUESTION 6
An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.
B. TCP half close.
C. TCP time wait.
D. TCP session time to live.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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.



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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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 IP address 192.168.12.232

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Examine the following partial outputs from two routing debug commands; then answer the question below.

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Examine the following partial outputs from two routing debug commands; then answer the question below.

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0
gwy=10.200.1.254 dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=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=253 type=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, port1
            [10/0] via 10.200.2.254, port2, [10/0]
c    10.0.1.0/24 is directly connected, port3
c    10.200.1.0/24 is directly connected, port1
c    10.200.2.0/24 is directly connected, port2
```


Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/2075/fortigate-wanopt-cache-proxy-524.pdf

QUESTION 12
Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://help.fortinet.com/fadc/4-2-2/cli/index.html#page/FortiADC_CLI_Reference/diagnose_debug_application.html

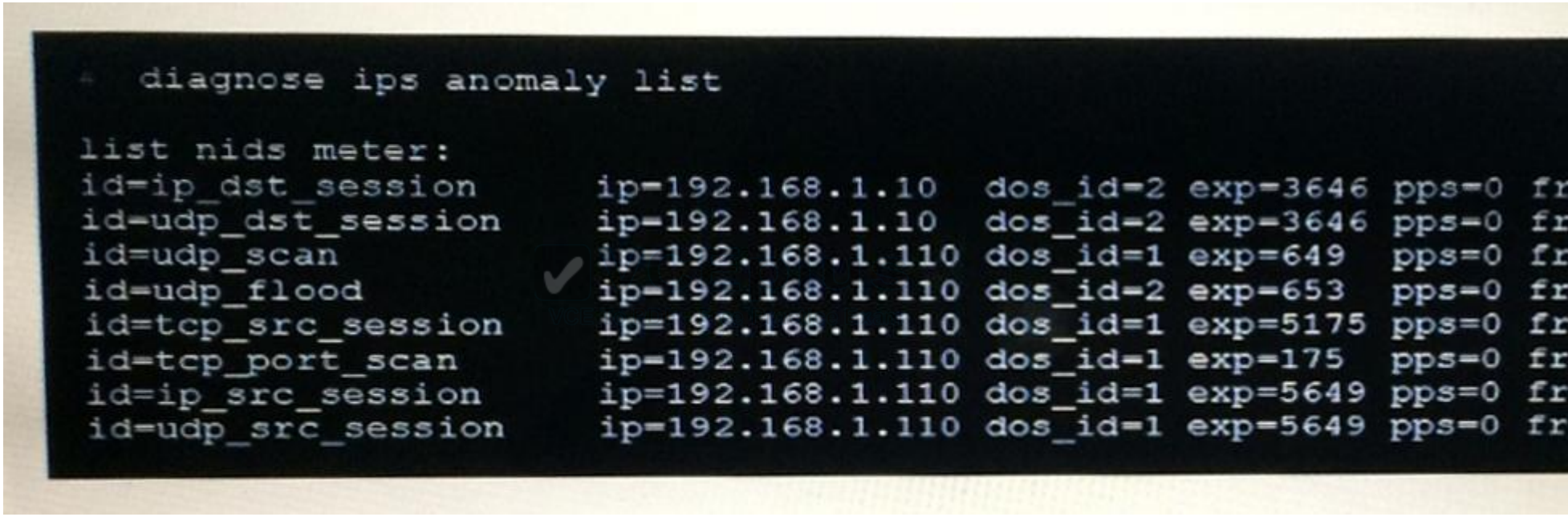
QUESTION 13
An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit's session to indicate that it has been synchronized to the secondary unit?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.



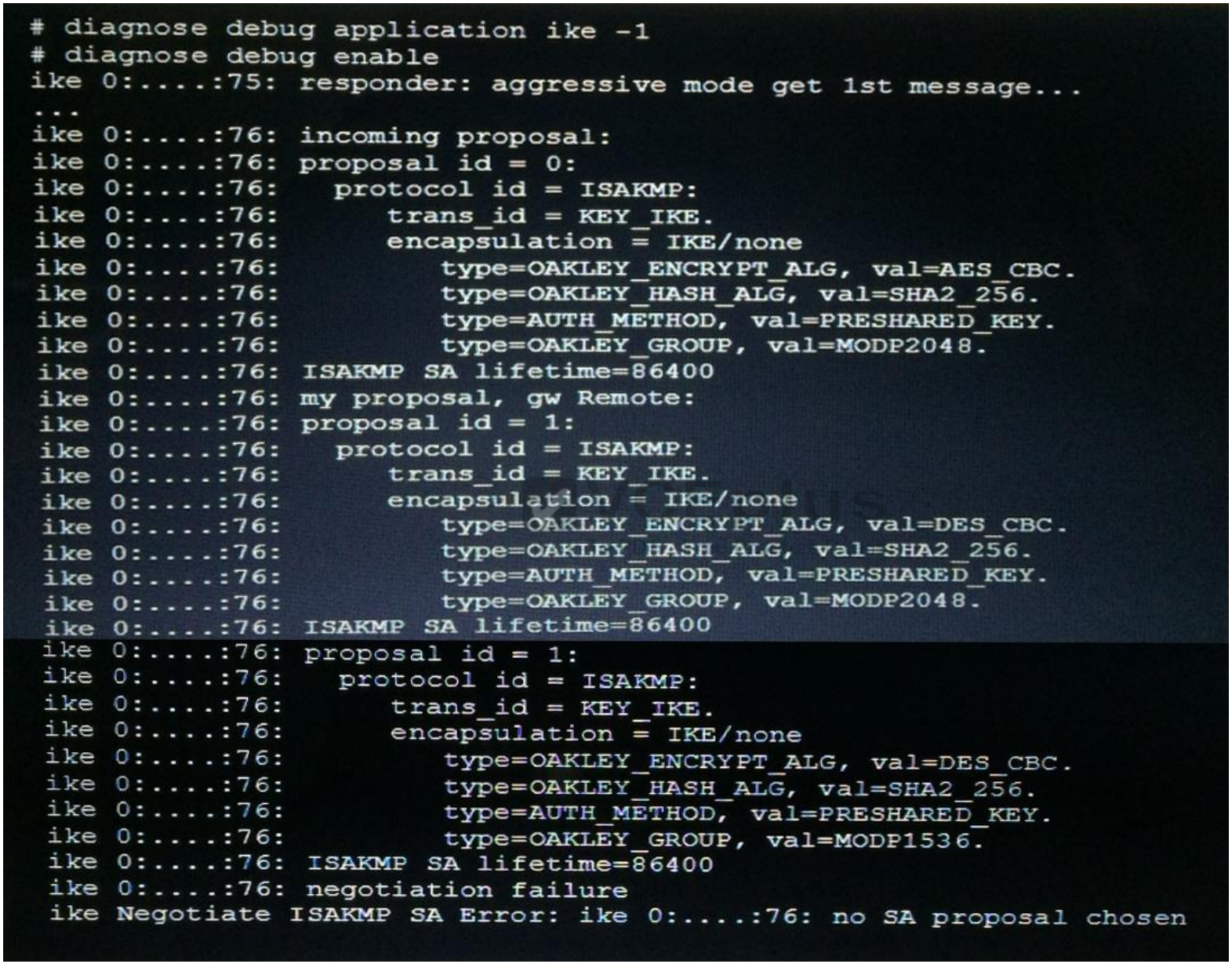
Which IP addresses are included in the output of this command?

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.



```
# diagnose debug application ike -1
# diagnose debug enable
ike 0:....:75: responder: aggressive mode get 1st message...
...
ike 0:....:76: incoming proposal:
ike 0:....:76: proposal id = 0:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:     trans_id = KEY_IKE.
ike 0:....:76:     encapsulation = IKE/none
ike 0:....:76:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:....:76:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: my proposal, gw Remote:
ike 0:....:76: proposal id = 1:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:     trans_id = KEY_IKE.
ike 0:....:76:     encapsulation = IKE/none
ike 0:....:76:       type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0:....:76:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: proposal id = 1:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:     trans_id = KEY_IKE.
ike 0:....:76:     encapsulation = IKE/none
ike 0:....:76:       type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0:....:76:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:       type=OAKLEY_GROUP, val=MODP1536.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:....:76: no SA proposal chosen
```

Why didn't the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.
B. The remote gateway's Phase-2 configuration does not match the local gateway's phase-2 configuration.
C. The remote gateway's Phase-1 configuration does not match the local gateway's phase-1 configuration.
D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*    0.0.0.0/0  [10/0] via 10.200.1.254, port1
C    10.200.1.0/24  is directly connected, port1
S    192.168.0.0/16  [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
    set as 65500
    set router-id 10.200.1.1
    set network-import-check enable
    set ebgp-miltipath disable
        config neighbor
            edit "10.200.3.1"
                set remote-as 65501
            next
        end
        config network
            edit1
```

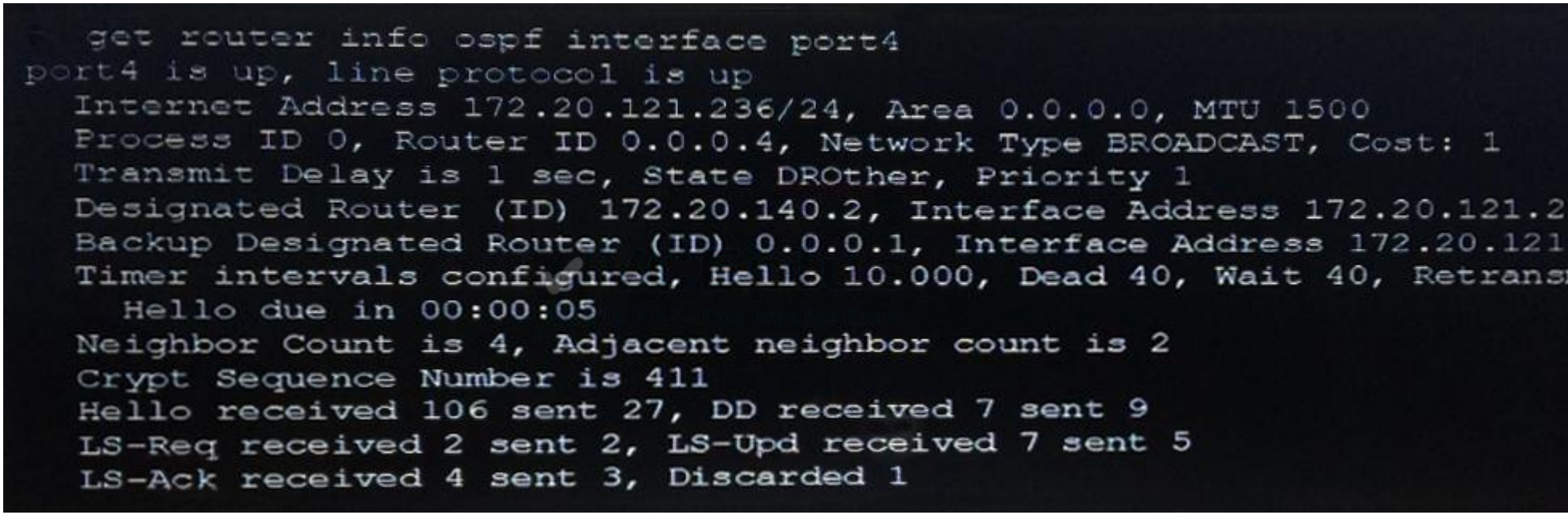

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Examine the output of the 'get router info ospf interface' commsnd shown in the exhibit; then answer the question below.



Which statements are true regarding the above output? (Chosse 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 nerwork.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug.

```
diagnose debug application ike -1
diagnose debug enable
```

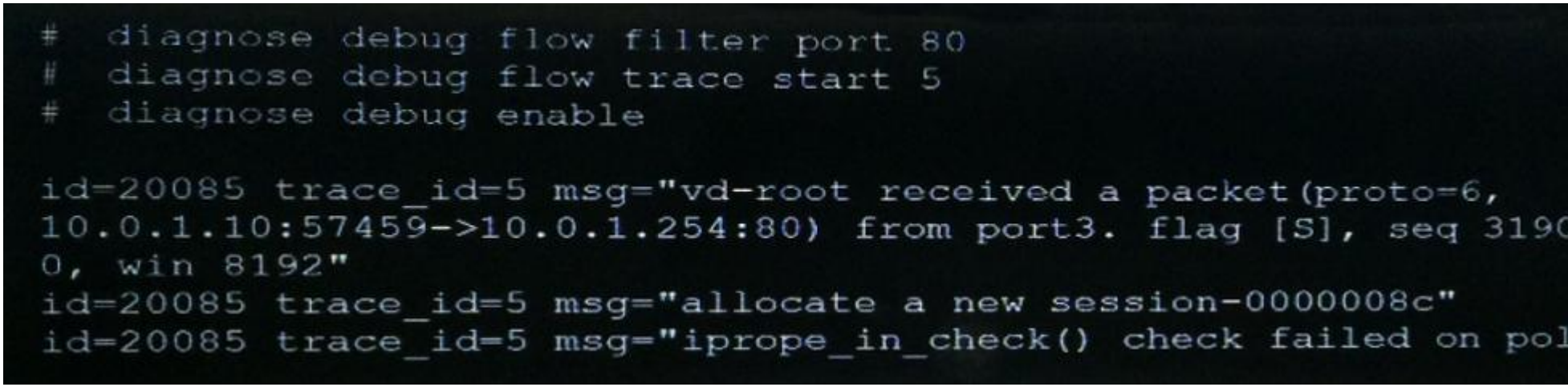
In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

A. Phase 1; IKE mode configuration; XAuth; phase 2.
B. Phase 1; XAuth; IKE mode configuration; phase 2.
C. Phase 1; XAuth; phase 2, IKE mode configuration.
D. Phase 1; IKE mode configuration; phase 2; XAuth.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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:



Based on the error displayed by the debug flow, which are valid reasosns 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://gembuls.wordpress.com/2013/07/03/how-to-avoid-fortigate-entered-conserve-mode/

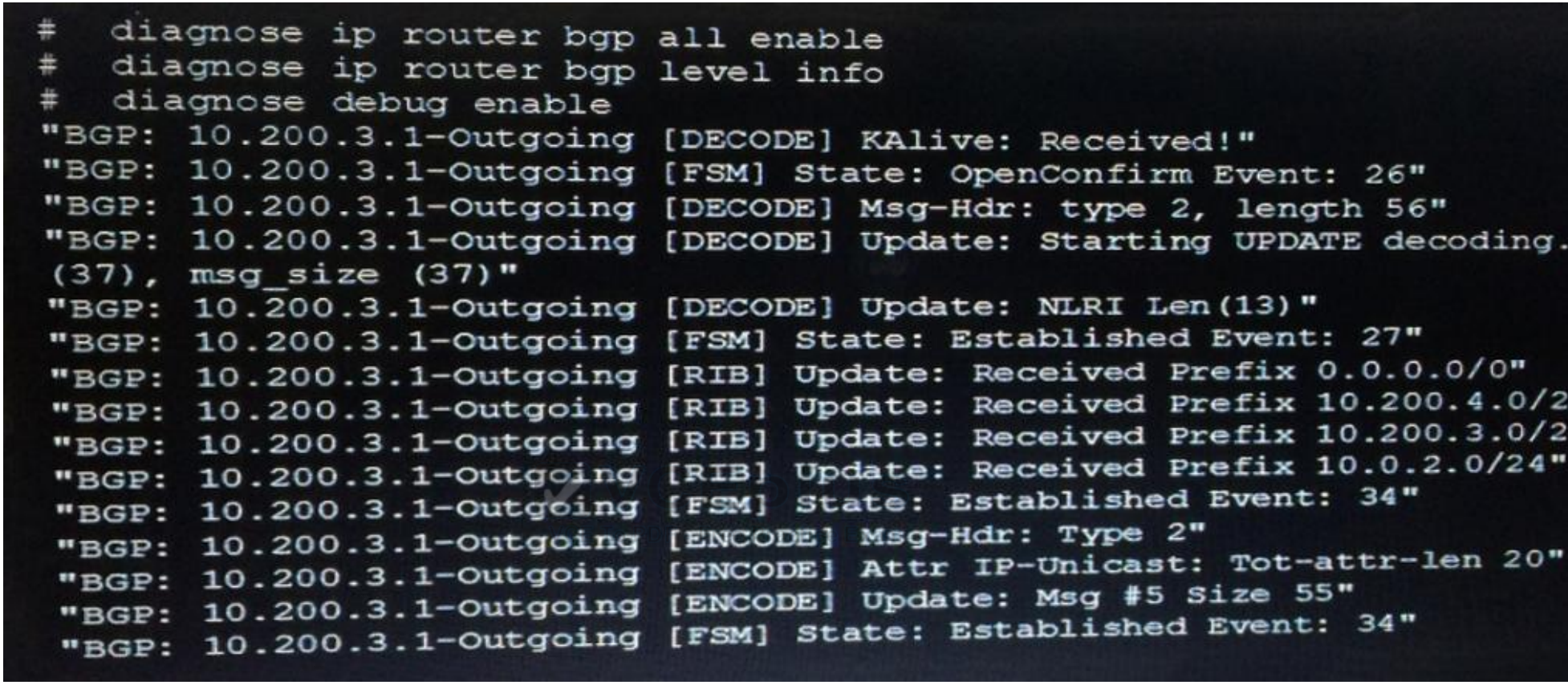
QUESTION 22
An administrator has configured a FortiGate device with two VDOMs: `root` and `internal`. The administrator has also created an inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routers to the other VDOM via OSPF through the inter-VDOM link. What 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.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:



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

A. BGP peers have successfully interchanged *Open* and *Keepalive* messages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer is *OpenConfirm*.
D. The state of the remote BGP peer will go to *Connect* after it confirms the received prefixes.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Examine the following traffic log; then answer the question below.

```
date-20xx-02-01 time=19:52:01 devname=master device_id="xxxxxxx" log_id=0100020007 type=event  subtype=system
pri critical vd=root service=kernel status=failure msg="NAT port is exhausted."
```

What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.
B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
C. FortiGate does not have any available NAT port for a new connection.
D. The limit for the maximum number of entries in the NAT port table has been reached.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference: