Fortinet.Premium.NSE7_EFW-7.0.30q - DEMO

Number: NSE7_EFW-7.0
Passing Score: 800
Time Limit: 120 min

Exam Code: NSE7_EFW-7.0
Exam Name: Fortinet NSE 7 - Enterprise Firewall 7.0
Website: https://VCEup.com/
Team-Support: Support@VCEup.com

QUESTION 1
Examine the IPsec configuration shown in the exhibit; then answer the question below.

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: diagnose vpn ike log-filter src-addr4 10.0.10.1 diagnose debug application ike -1 diagnose debug enable The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

A. The IKE real time shows the phases 1 and 2 negotiations only. It does not show any more output once the tunnel is up.
B. The log-filter setting is set incorrectly. The VPN's traffic does not match this filter.
C. The IKE real time debug shows the phase 1 negotiation only. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
D. The IKE real time debug shows error messages only. If it does not provide any output, it indicates that the tunnel is operating normally.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
B. SIP ALG supports SIP HA failover; SIP helper does not.
C. SIP ALG supports SIP over IPv6; SIP helper does not.
D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
A FortiGate device has the following LDAP configuration:

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

The administrator executed the 'dsquery' command in the Windows LDAp server 10.0.1.10, and got the following output:
>dsquery user –samid administrator
"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab"
Based on the output, what FortiGate LDAP setting is configured incorrectly?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 4
A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fsso list' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

A. The user student must not be listed in the CA's ignore user list.
B. The user student must belong to one or more of the monitored user groups.
C. The student workstation's IP subnet must be listed in the CA's trusted list.
D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

QUESTION 5
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:
Explanation: http://docslegacy. fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&fil e=CLI_get_Commands.58.25.html
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table.
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.
The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-ofsequence packet.

QUESTION 6
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.

Correct Answer: BC
Section: (none)
Explanation

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

QUESTION 7
Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General Organizations
   49 Business
   50 Information and Computer Security
   51 Government and Legal Organizations
   52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking
B. General organization.
C. Business.
D. Information technology.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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).

QUESTION 9
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

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

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

Total number of neighbors 3
```

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

A. BGP state of the peer 10.125.0.60 is Established.

B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixes.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
.....
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn't match the sniffer filter.
B. Number of total packets dropped by the FortiGate.
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=11655

QUESTION 11
A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878  n_dns_fails= 2  n_dns_timeout=875
n_dns_success=0

n_snd_retries=0  n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

A. The connectivity between the FortiGate unit and the DNS server.
B. The connectivity between the client workstations and the DNS server.
C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
D. That DNS service is enabled in the explicit web proxy interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 13
Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; than answer the question below.

```
#diagnose sys session list expectation

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

Which statement is true regarding the session in the exhibit?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
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.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
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. Phase1; IKE mode configuration; XAuth; phase 2.
B. Phase1; XAuth; IKE mode configuration; phase2.
C. Phase1; XAuth; phase 2; IKE mode configuration.
D. Phase1; IKE mode configuration; phase 2; XAuth.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet_Processing.htm

QUESTION 16
Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

A. Group ID.
B. Group name.
C. Session pickup.
D. Gratuitous ARPs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

QUESTION 17
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:
Explanation:

QUESTION 18
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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 19
Examine the output of the 'get router info ospf neighbor' command shown in the exhibit; then answer the question below.

```
# 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  wan1
0.0.0.2         1   Full/ -         00:00:36    172.16.1.2    ToRemote
```

Which statements are true regarding the output in the exhibit? (Choose two.)
Refer to the exhibit, which shows the output of a debug command.
Which statement about the output is true?

A. TheOSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the war. I network.
B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
C. The local FortiGate is the designated router for the wan1 network.
D. The interface ToRemote is a point-to-point OSPF network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

QUESTION 20
A FortiGate has two default routes:

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

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

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

A. A process crash.
B. Configuration changes.
C. Changes in the status of any of the FortiGuard licenses.
D. System entering to and leaving from the proxy conserve mode.

Correct Answer: AD
Section: (none)

Explanation

Explanation/Reference:
Explanation: diagnose debug crashlog read 275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated 276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated 277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated 278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel 279: 2014-08-06 11:05:47 enters conserve mode" 280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages" 281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode" 282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201 283: 2014-08-06 13:07:16 marginexit=302

QUESTION 22
Examine the following partial outputs from two routing debug commands; then answer the question below:

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103

QUESTION 23
A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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:

Explanation:
The synced sessions have the ‘synced’ flag. The command ‘diag sys session list’ can be used to see the sessions on the member, with the associated flags.

QUESTION 25
Examine the output of the ‘get router info bgp summary’ command shown in the exhibit; then answer the question below.

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

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

Total number of neighbors 1
```

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4

QUESTION 26
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

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

Why didn't the tunnel come up?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
A FortiGate device has the following LDAP configuration:

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

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

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

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

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=13141

QUESTION 29
Examine the output from the 'diagnose vpn tunnel list' command shown in the exhibit; then answer the question below.

```
#diagnose vpn tunnel list
name-Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2: 64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refcnt=8 ilast=4 olast=4
stat: rxp=104 txp=8 rxb=27392 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt: mode=silent draft=32 interval= 10 remote_port=64916
proxyid= DialUp proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0.-255.255.255.255:0
  dst: 0:10.0.10.10.-10.0.10.10:0
  SA: ref=3 options= 00000086 type=00 soft=0 mtu=1422 expire =42521
replaywin=2048 seqno=9
  life: type=01 bytes=0/0 timeout= 43185/43200
  dec: spi=cb3a632a esp=aes key=16  7365e17a8fd555ec38bffa47d650c1a2
       ah=sha1 key=20  946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
  enc: spi=da6d28ac  esp=aes  key=16  3dcf44ac7c816782ea3d0c9a977ef543
       ah=sha1 key=20   7cfde587592fc4635ab8db8ddf0d851d868b243f
dec:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

Which command can be used to sniffer the ESP traffic for the VPN DialUP_0?

A. diagnose sniffer packet any ‘port 500’
B. diagnose sniffer packet any ‘esp’
C. diagnose sniffer packet any ‘host 10.0.10.10’
D. diagnose sniffer packet any ‘port 4500’

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NAT-T is enabled. natt: mode=silent
Protocol ESP is used. ESP is encapsulated in UDP port 4500 when NAT-T is enabled. natt: mode=silent means IPSec is behind NAT (NAT traversal)
https://kb.fortinet.com/kb/documentLink.do?externalID=FD48755

QUESTION 30
View the central management configuration shown in the exhibit, and then answer the question below.

```
config system central-management
   set type fortimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
         set server-type update
         set server-address 10.0.1.243
      next
      edit 3
         set server-type rating
         set server-address 10.0.1.244
      next
   end
   set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

A. 10.0.1.240
B. One of the public FortiGuard distribution servers
C. 10.0.1.244
D. 10.0.1.242

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: