Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
Refer to the exhibit, which shows 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 inervals 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 send 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 output are true? (Choose two.)

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

Answer: AB

Explanation:
Area 0.0.0.0 is the backbone area.

NEW QUESTION 2
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

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

Why didn't the tunnel come up?

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

Answer: C

NEW QUESTION 3
Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.
B. When executed on the Device Database, you must use the installation wizard to apply the changes 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.

Answer: BD

Explanation:
CLI scripts can be run in three different ways:Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.
Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.
Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

NEW QUESTION 4
Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

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

Answer: CDE

Explanation:
A configured static route only goes to routing table from routing database when all the following are met :
≫ The outgoing interface is up
≫ There is no other matching route with a lower distance
≫ The link health monitor (if configured) is successful
≫ The next-hop IP address belongs to one of the outgoing interface subnets

NEW QUESTION 5
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 6
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 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 7
Refer to exhibit, which contains 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 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 8

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.

Answer: C

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

NEW QUESTION 9

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 10

Refer to the exhibit, which contains the debug output of diagnose dvm device list.

```
FMG-VM64# diagnose dvm device list
There are currently 1 devices/vdoms managed:
TYPE    OID   SN       HA      IP          NAME          ADOM      IPS  FIRMWARE
fmg/    217   FGVM01…  -    10.200.1.1 Local-FortiGate  My_ADOM 15.0.0831 6.0 MR4 (1579)
faz enabled                                                   (regular)

      |-  STATUS: db: modified; conf: in sync; cond: pending; dm: retrieved;  conn: up

      |- vdom: [3] root flags:0 adom:My_ADOM pkg: [imported] Local-FortiGate_root
```

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

A. ADOMs are disabled on the FortiManager
B. The FortiGate configuration is in sync with latest running revision history.
C. There are pending device-level changes yet to be installed on Local-FortiGate.
D. The policy package has been modified for Local-FortiGate.

Answer: BC

NEW QUESTION 10
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 12
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. Neighbor range
B. Route reflector
C. Next-hop-self
D. Neighbor group

Answer: B

Explanation:
Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routers learned from one peer to the other peers. If you configure route reflectors, you dont' need to create a full mesh IBGP network. All clients in a cluster only talck to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

NEW QUESTION 15
In which two states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.
B. A TCP session waiting for FIN ACK.
C. A UDP session with packets sent and received.
D. A UDP session with only one packet received.

Answer: AD

NEW QUESTION 17
View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
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 tuples=2
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=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
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
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: B

NEW QUESTION 22
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 25
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 26
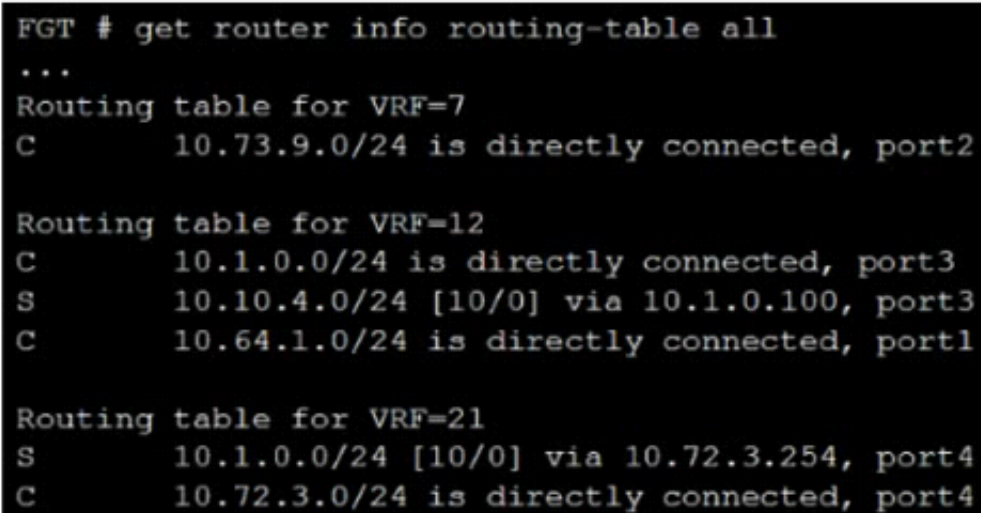Which two statements about an auxiliary session are true? (Choose two.)

A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.
C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.
D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

Answer: CD

NEW QUESTION 27
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 28
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "portl" set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

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

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

What is causing the IPsec problem in the phase 1 ?

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

Answer: C

NEW QUESTION 32
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 seqno=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'

Answer: D

Explanation:
NAT-T is enabled. natt: mode=silentProtocol 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

NEW QUESTION 36
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 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=20000ms 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: 0:10.1.2.0/255.255.255.0:0
     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-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.

Answer: AC

NEW QUESTION 40
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 44
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.

Answer: AD

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

NEW QUESTION 47
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 52
Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

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

Answer: AC

NEW QUESTION 54
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_EFW-7.0 Practice Exam Features:

* NSE7_EFW-7.0 Questions and Answers Updated Frequently

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

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

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

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