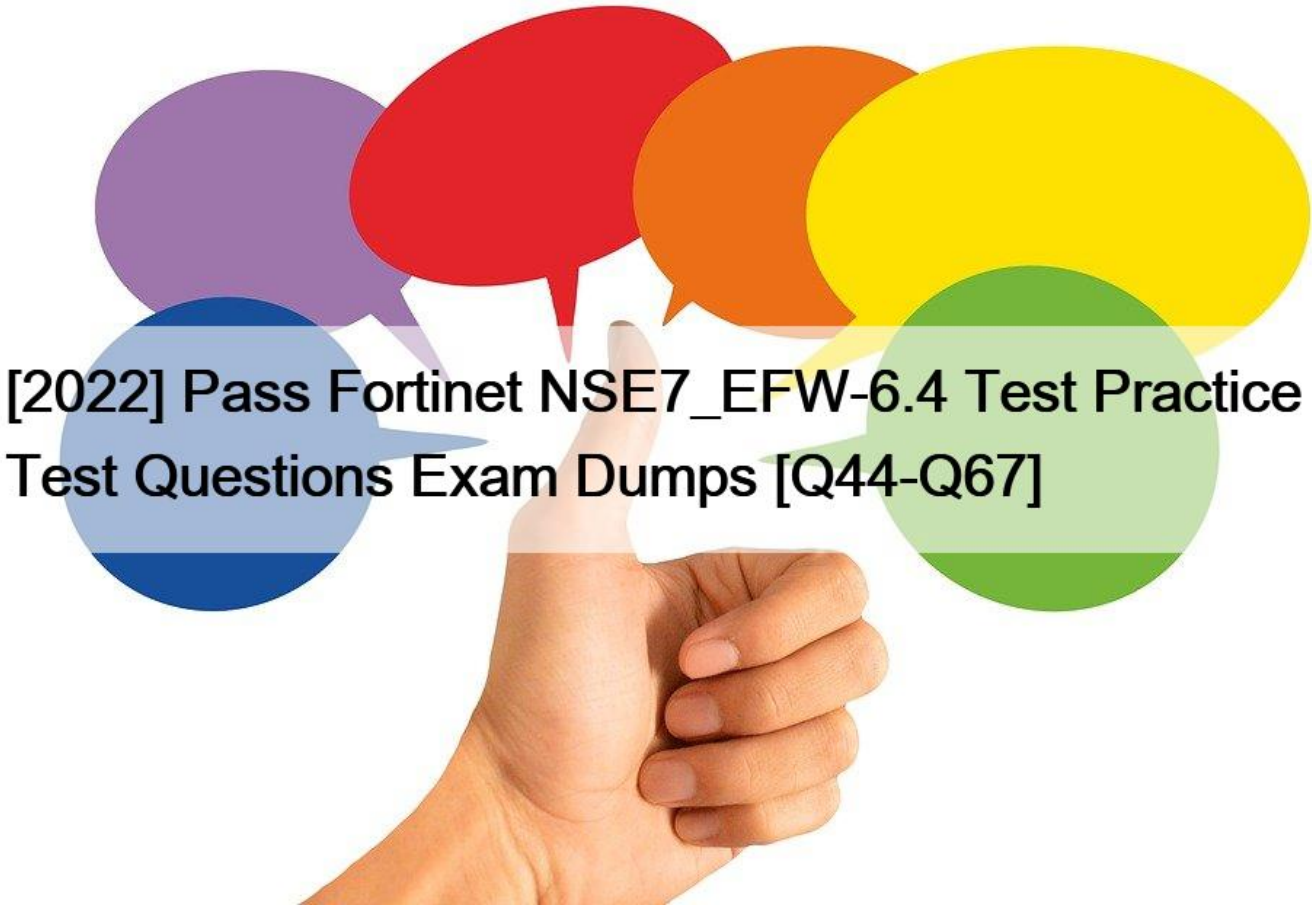
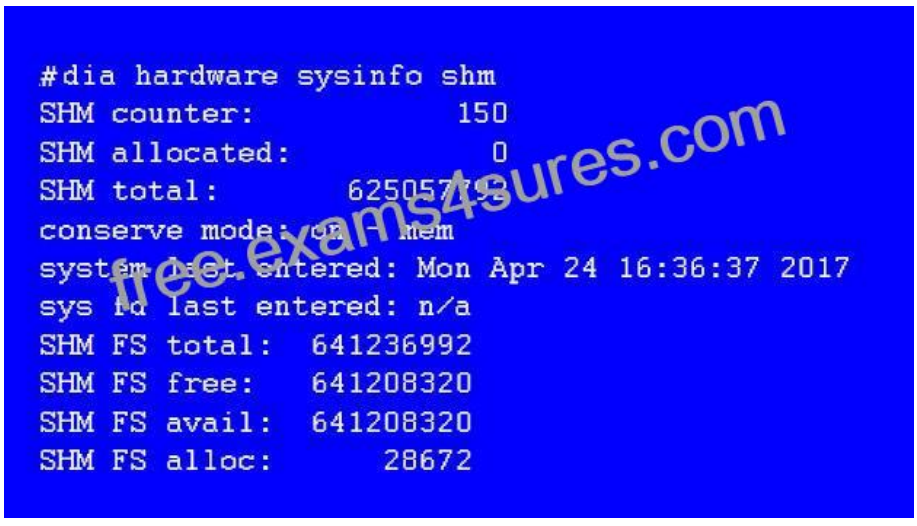
[2022 Pass Fortinet NSE7_EFW-6.4 Test Practice Test Questions Exam Dumps [Q44-Q67



[2022] Pass Fortinet NSE7_EFW-6.4 Test Practice Test Questions Exam Dumps
Verified NSE7_EFW-6.4 dumps Q&As - NSE7_EFW-6.4 dumps with Correct Answers

NO.44 View the exhibit, which contains the output of a debug command, and then answer the question below.



free.exams4sures.com

What statement is correct about this FortiGate?
* It iscurrently in system conserve mode because of high CPU usage.
* It is currently in FD conserve mode.
* It is currently in kernel conserve mode because of high memory usage.
* It is currently in system conserve mode because of high memory usage.

NO.45 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?
* TCP half open.
* TCP half close.
* TCP time wait.
* TCP session time to live.

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=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.

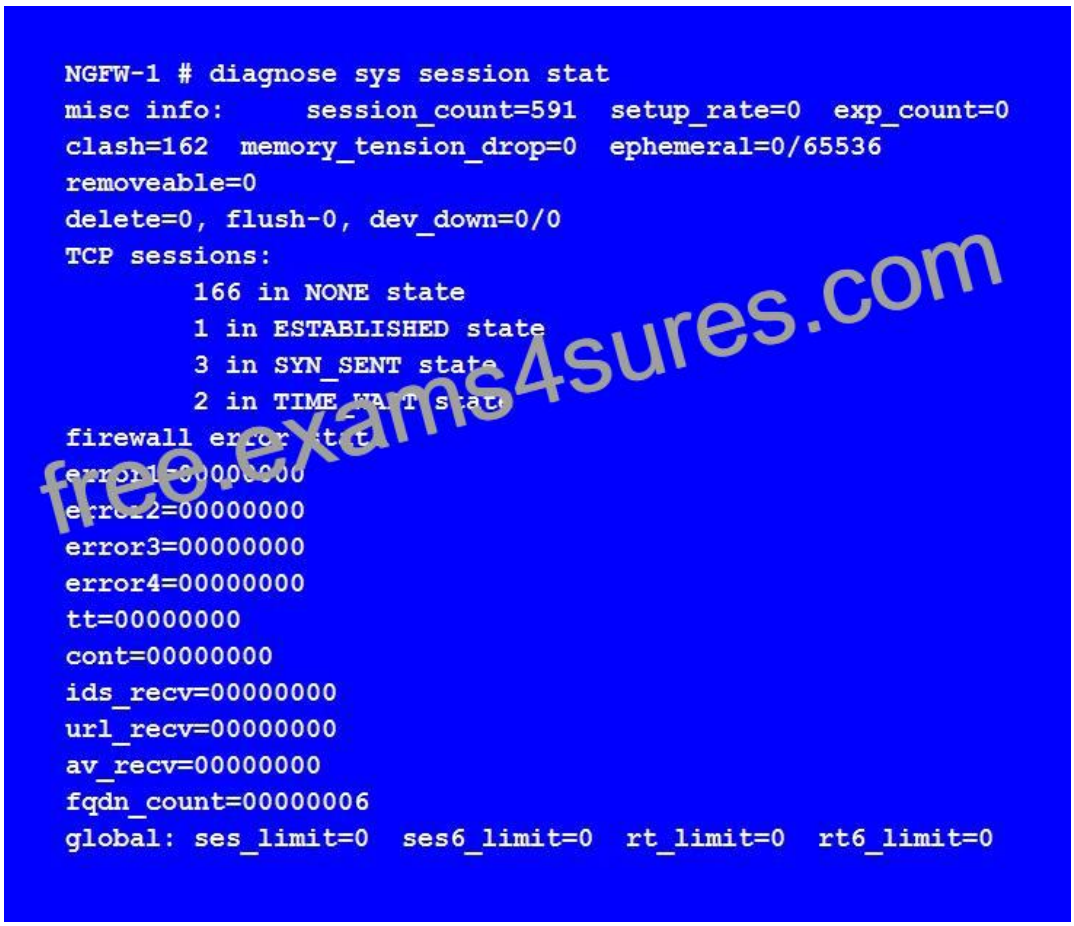
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.

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-of-sequence packet.

NO.46 Whendoes a RADIUS server send an Access-Challenge packet?
* The server does not have the user credentials yet.
* The server requires more information from the user, such as the token code for two-factor authentication.
* The user credentials are wrong.
* The user account is not found in the server.

NO.47 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?
* Forces the former primary device to shut down all its non-heartbeat interfaces forone second while the failover occurs.
* Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
* Sends a link failed signal to all connected devices.
* Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

NO.48 View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.



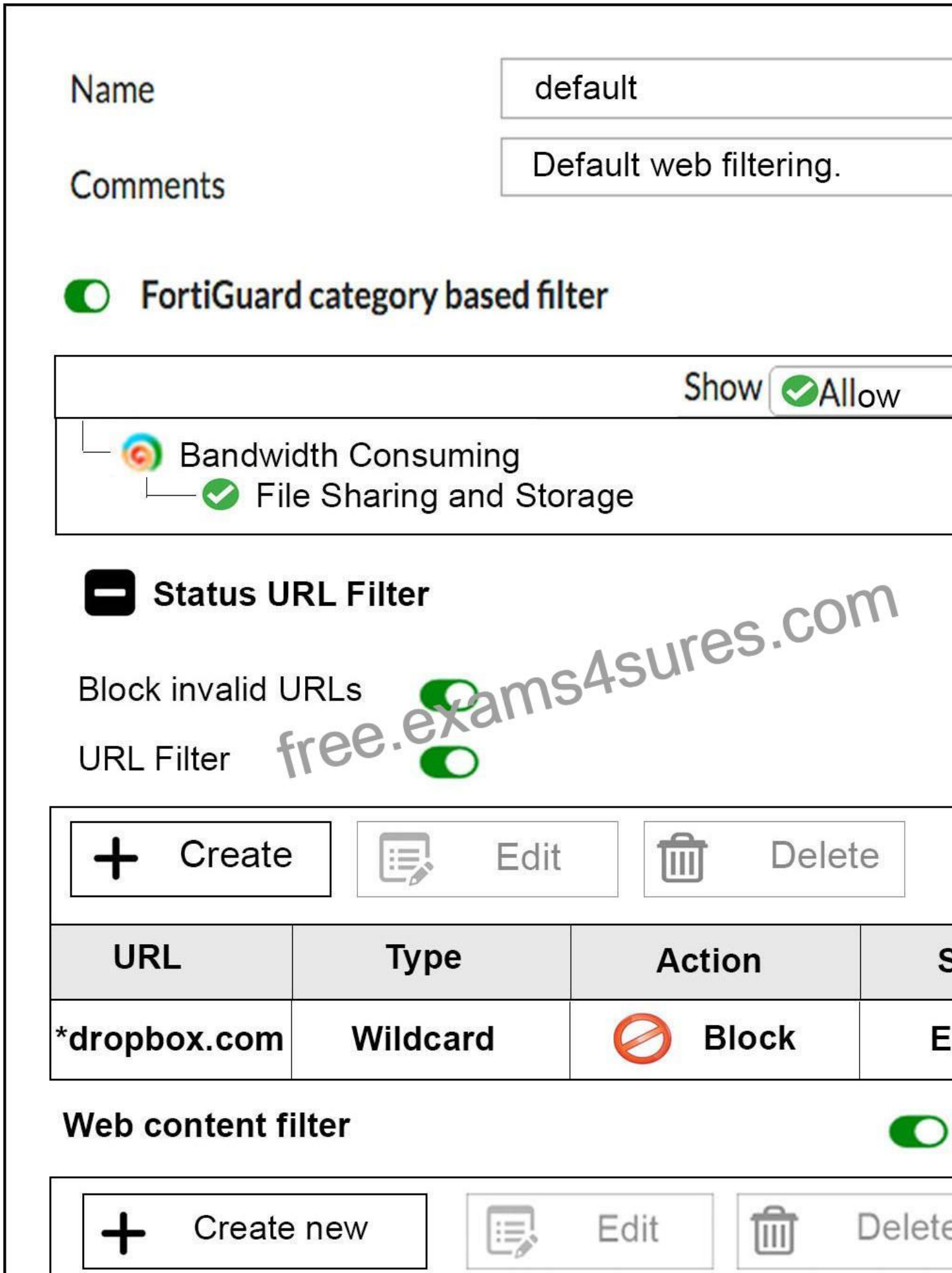
free.exams4sures.com

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

* There are 0 ephemeral sessions.
* All the sessions in the session table are TCP sessions.
* No sessions have been deleted because of memory pages exhaustion.
* There are 166 TCP sessions waiting to complete the three-way handshake.

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578

NO.49 View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.



free.exams4sures.com

Which action willFortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

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

Explanation

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

NO.50 View the exhibit, which contains the output of a web diagnose command, and then answer the question below.

```
# diagnose webfilter fortiguard statistics list

Raring Statistics:
==================================
DNS filures                    :    273
DNS lookups                    :    280
Data send failures             :      0
Data read failures             :      0
Wrong package type             :      0
Hash table miss                :      0
Unknown server                 :      0
Incorrect CRC                  :      0
Proxy requests failures        :      0
Request timeout                :      1
Total requests                 :   2409
Requests to FortiGuard servers :    118
Server errored responses       :      0
Relayed ratin                  :      0
Invalid profile                :      0

Allowed                        :   1021
Blocked                        :   3909
Logged                         :   3927
Blocked Errors                 :    565
Allowed Errors                 :      0
Monitors                       :      0
Authenticates                  :      0
Warnings                       :     18
Ovrd request timeout           :      0
Ovrd send failures             :      0
Ovrd read failures             :      0
Ovrd errored responses         :      0
...
```

```
# diagnose webfilter fortiguard statistics list

Cache Statistics:
======================
Maximum memory                 :      0
Memory usage                   :      0

Nodes                          :      0
  Leaves                       :      0
  Prefix nodes                 :      0
  Exact nodes                  :      0

Requests                       :      0
Misses                         :      0
Hits                           :      0
  Prefix hits                  :      0
  Exact hits                   :      0

No cache directives            :      0
Add after prefix               :      0
Invalid DB put                 :      0
DB updates                     :      0

Percent full                   :     0%
  Branches                     :     0%
  Leaves                       :     0%
    Prefix nodes               :     0%
    Exact nodes                :     0%

Miss rate                      :     0%
Hit rate                       :     0%
  Prefix hits                  :     0%
  Exact hits                   :     0%
```

free.exams4sures.com

Which one of the following statements explains why the cache statistics are all zeros?

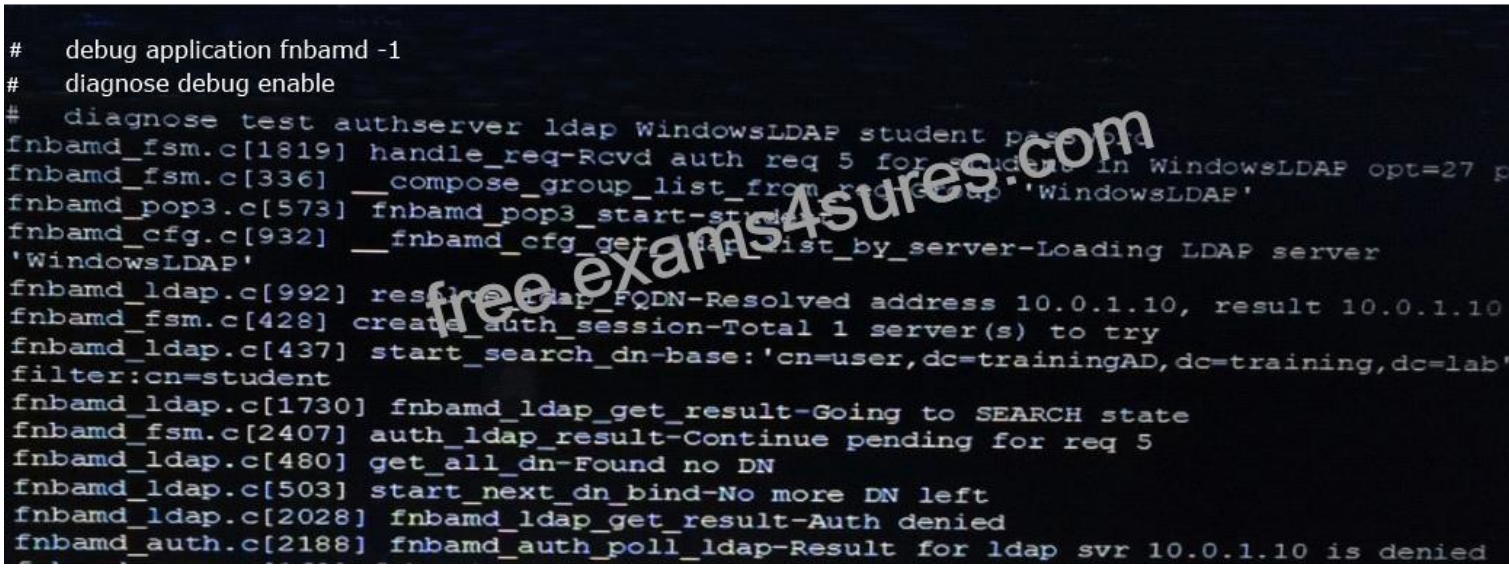
* Theadministrator has reallocated the cache memory to a separate process.
* There are no users making web requests.
* The FortiGuard web filter cache is disabled in the FortiGate’s configuration.
* FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

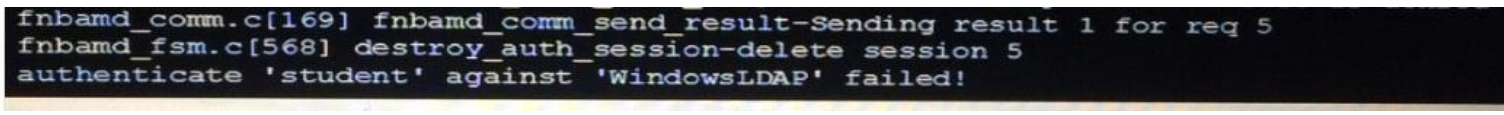
NO.51 A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the ‘diagnose debug authd fsso list’ command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)
* The user student must not be listed in the CA’s ignore user list.
* The user student must belong to one or more of the monitored user groups.
* The student workstation’s IP subnet must be listed in the CA’s trusted list.
* At least one of thestudent’s user groups must be allowed by a FortiGate firewall policy.

Explanation

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

NO.52 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?
* User student is not found in the LDAP server.
* User student is using a wrong password.
* The FortiGate has been configured with the wrong password for the LDAP administrator.
* The FortiGate has been configured with the wrong authentication schema.

NO.53 An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs thedebug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

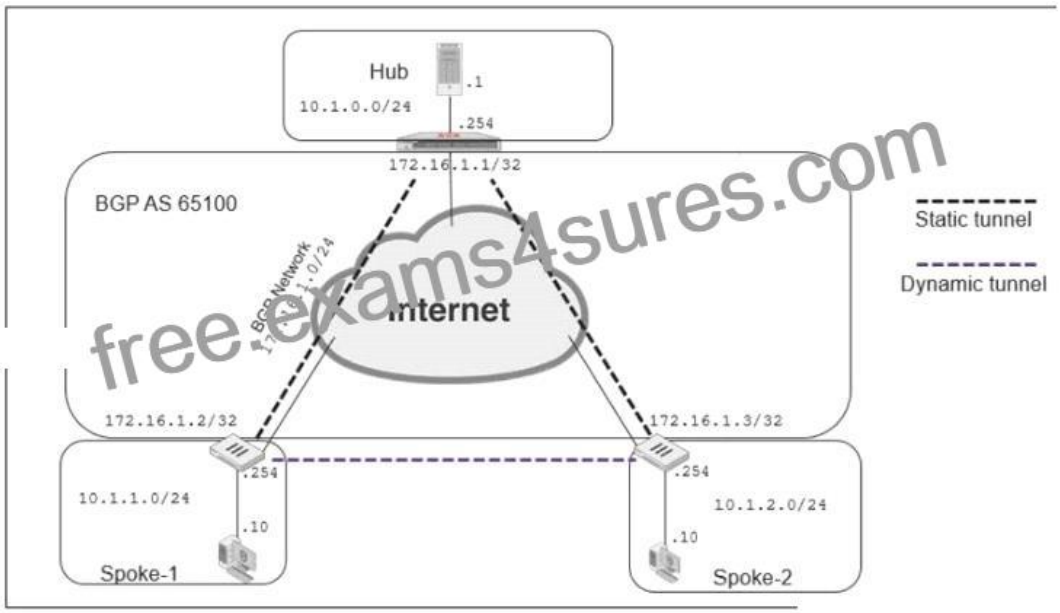
```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy
```

free.exams4sures.com

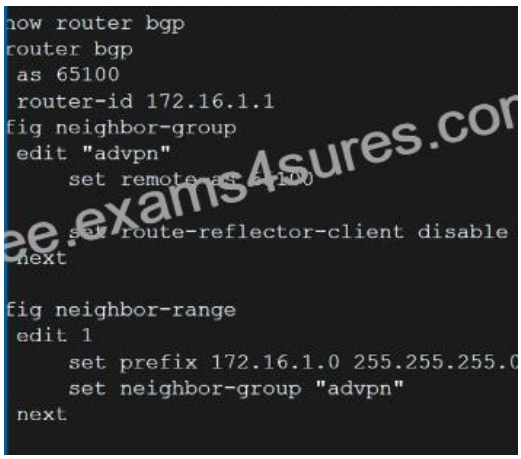
Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

* HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
* Redirection of HTTP to HTTPS administrative access is disabled.
* HTTP administrative access is configured with a port number different than 80.
* The packet is denied because of reverse path forwarding check.

NO.54 Exhibits:



free.exams4sures.com



Refer to the exhibits, which contain the network topology and BGP configuration for a hub.

An administrator is trying to configure ADVPN with a hub-spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however, the spokes are not receiving route information from each other.

What change must the administrator make to the hub BGP configuration so that the routes learned by one spoke are forwarded to the other spokes?

* Configure an individual neighbor and remove neighbor-range configuration.
* Configure the hub as a route reflector client.
* Change the router id to 10.1.0.254.
* Make the configuration of remote-as different from the configuration of local-as.

NO.55 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?

* cnid.
* username.
* password.
* dn.

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

NO.56 View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
     diagnose sys session list expectation

session info: proto=6 proto_state-00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
ha_id-0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply-0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir-org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook-pre dir-org act-noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

free.exams4sures.com

What statements are correct regarding the output? (Choose two.)

* This is anexpected session created by a session helper.
* Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
* Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
* This is an expected session created by an application control profile.

NO.57 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
```

free.exams4sures.com

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?

* TheOSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the war. l network.
* The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.

* The local FortiGate is the designated router for the wan1 network.
* The interface ToRemote is a point-to-point OSPF network.
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

NO.58 Examine the IPsec configuration shown in the exhibit; then answer the question below.

ee.exams4sures.cor

An administrator wants to monitor the VPN by enabling theIKE 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 beinginterchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn’t there any output?
* The IKE real time shows the phases 1 and 2 negotiations only. It does not show any more output once the tunnel is up.
* The log-filter setting is set incorrectly. The VPN’s traffic does not match this filter.
* 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.
* The IKE real time debug shows error messages only. If it does not provide any output, it indicates that the tunnel is operating normally.

NO.59 Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:    protocol id = ISAKMP.
ike 0: Remotesite:3:         trans_id = KEY_IKE.
ike 0: Remotesite:3:              encapsulation = IKE/none.
ike 0: Remotesite:3:                  type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:                  type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:                  type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:                  type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

free.exams4sures.com

Which two statements about this debug output are correct? (Choose two.)

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

NO.60 Examine the output ofthe ‘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
```

free.exams4sures.com

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?
* The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
* The TCP session for the BGP connection to 10.200.3.1 is down.
* The local peer has received the BGP prefixed from the remote peer.
* The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Explanation

http://www.ciscopress.com/articles/article.asp?p=2756480

NO.61 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?
* Group ID.
* Group name.
* Session pickup.
* Gratuitous ARPs.

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

NO.62 Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 843516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concervemode: 0
shm last entered: n/a
system last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912
SHM FS alloc: 7110656
```

Which of the following statements are true regarding the above outputs? (Choose two.)
* The unit is running a 32-bit FortiOS
* The unit is in kernel conserve mode
* The Cached value is always the Active value plus the Inactive value
* Kernel indirectly accesses the low memory (LowTotal) through memorypaging

NO.63 View the exhibit, which contains the output of get sys ha status, and then answer the question below.

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
  <2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
  <2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649(updated 1 seconds ago): in-sync
  FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
  FGVM010000077649(updated 1 seconds ago):
     sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
  FGVM010000077650(updated 0 seconds ago):
     sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
  FGVM010000077649(updated 1 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
  FGVM010000077650(updated 0 seconds ago):
     port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW        , FGVM010000077649
Slave : NGFW-2      , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM0100000077649
Slave :1 FGVM0100000077650
```

free.exams4sures.com

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

* The slave configuration is not synchronized with the master.
* The HA management IP is 169.254.0.2.
* Master is selected because it is the only device in the cluster.
* port 7 is used the HA heartbeat on all devices in the cluster.

NO.64 View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

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

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

free.exams4sures.com

Which of the following statements is true regarding this output?
* The requested URL belongs to category ID 255.
* The server hostname Is training, fortinet.com.
* FortiGate found the requested URL in its local cache.
* This web request was inspected using the ftgd-allow web filler profile.

NO.65 View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
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
```

free.exams4sures.com

Which ofthe following statements about the exhibit are true? (Choose two.)
* The local router’s BGP state is Established with the 10.125.0.60 peer.
* Since the counters were last reset; the 10.200.3.1 peer has never been down.
* The local router has received atotal of three BGP prefixes from all peers.
* The local router has not established a TCP session with 100.64.3.1.

NO.66 Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?
* Diagnose debug application radius -1.
* Diagnose debug application fnbamd -1.
* Diagnose authd console -log enable.
* Diagnose radius console -log enable.

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

NO.67 What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?
* av-failopen
* mem-failopen
* utm-failopen
* ips-failopen

Explanation

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideration

NSE7_EFW-6.4 certification guide Q&A from Training Expert Exams4sures:
https://www.exams4sures.com/Fortinet/NSE7_EFW-6.4-practice-exam-dumps.html]