Fortinet

Exam Questions NSE7

NSE7 Enterprise Firewall - FortiOS 5.4

NEW QUESTION 1
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 2
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.

Answer: A

NEW QUESTION 3
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.

Answer: AB

NEW QUESTION 4
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.

Answer: A

NEW QUESTION 5
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.182:80(10.200.1.1:65464
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/(0/0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement is correct regarding the output?

A. This session is for HA heartbeat traffic.
B. This session is synced with the slave unit.
C. The inspection of this session has been offloaded to the slave unit.
D. This session cannot be synced with the slave unit.

Answer: B

NEW QUESTION 6
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

Answer: B

NEW QUESTION 7
In which of the following 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: BC

NEW QUESTION 8
View the exhibit, which contains the output of a real-time debug, and then answer the question below.

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

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache.   URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

A. This web request was inspected using the root web filter profile.
B. FortiGate found the requested URL in its local cache.
C. The requested URL belongs to category ID 52.
D. The web request was allowed by FortiGate.

Answer: BC

NEW QUESTION 9
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 onl
B. It does not show any more output once the tunnel is up.
C. The log-filter setting is set incorrectl
D. The VPN's traffic does not match this filter.
E. The IKE real time debug shows the phase 1 negotiation onl
F. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
G. The IKE real time debug shows error messages onl
H. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: A

NEW QUESTION 10
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'

Answer: B

NEW QUESTION 10
A FortiGate's portl 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.

Answer: AD

NEW QUESTION 13
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 15
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 16
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.

Answer: BC

NEW QUESTION 21
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:

```
# 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 3190430861, ack
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 0, drop"
```

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 25
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.

Answer: D

NEW QUESTION 27
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.

Answer: AD

NEW QUESTION 29
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: AD

NEW QUESTION 33
.....

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 Practice Exam Features:

* NSE7 Questions and Answers Updated Frequently

* NSE7 Practice Questions Verified by Expert Senior Certified Staff

* NSE7 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year