NSE7_EFW Q&As

NSE7 Enterprise Firewall - FortiOS 5.4

Pass Fortinet NSE7_EFW Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse7_efw.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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

A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.

B. FortiGate limits the total number of simultaneous explicit web proxy users.

C. FortiGate limits the number of simultaneous sessions per explicit web proxy user. The limit CAN be modified by the administrator.

D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: C

QUESTION 2

View the global IPS configuration, and then answer the question below.

```
config ips global
    set fail-open disable
    set intelligent-mode disable
    set engine-count 0
    set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.

B. FortiGate will spawn IPS engine instances based on the system load.

C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.

D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Correct Answer: A

QUESTION 3

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_shape=
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=10.200.1.254/10.1.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.185:80(10.200.1.1:65464)
pos/ (before, after) 0/(0/0), 0/(0/0)
misc=0 policy_id=1 aut_info=0 chk_client_info=0 vd=0
serial=0000009B 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.

Correct Answer: B

QUESTION 4

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=3q
origin-shaper=q
reply-shaper=q
per-ip_shaper=q
ha_id=0'policy_dir=1'tunnel=/q
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)q
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=00000e9'tos=ff/ff'ips_view=0 app_list=0'app=0
dd type=0'dd_mode=0q
```

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: A

QUESTION 5

A FortiGate has two default routes:

```
config router static
   edit 1
     set gateway 10.200.1.254
     set priority 5
     set device "port1"
   next
   edit 2
     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 expire7 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-
>10.200.1.1:67907(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. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A

QUESTION 6

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

QUESTION 7

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.

Correct Answer: AD

QUESTION 8

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
```

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

A. This is an expected session created by a session helper.

B. 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.

C. 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.

D. This is an expected session created by an application control profile.

Correct Answer: AC

QUESTION 9

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.

Correct Answer: BC

QUESTION 10

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: 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_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=MODP1536.
ike 0:····: 76:ISAKMP SA lifetime=86400
ike 0:····: 76:negotiation failure
ike Negotiate ISAKMP SA Error:ike 0: ···: 76: no SA proposal chosen
```

Why didn\\'t the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.

B. The remote gateway\\'s Phase-2 configuration does not match the local gateway\\'s phase-2 configuration.

C. The remote gateway\\'s Phase-1 configuration does not match the local gateway\\'s phase-1 configuration.

D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: B

QUESTION 11

View the exhibit, which contains the output of a debug command, and then answer the question below.

```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:          0
SHM total:      625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total: 641236992
SHM FS free:  641208320
SHM FS avail: 641208320
SHM FS alloc:     28672
```

What statement is correct about this FortiGate?

A. It is currently in system conserve mode because of high CPU usage.

B. It is currently in FD conserve mode.

C. It is currently in kernel conserve mode because of high memory usage.

D. It is currently in system conserve mode because of high memory usage.

Correct Answer: D

QUESTION 12

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.

Correct Answer: AC

QUESTION 13

A FortiGate device has the following LDAP configuration: The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
config user ldap
    edit "WindowsLDAP"
        set server "10.0.1.10"
        set cnid "cn"
        set dn "cm=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
```

```
#diagnose debug application fnband -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fam.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]fnband_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_resuilt_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

QUESTION 14

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: C

QUESTION 15

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.

Correct Answer: A

Latest NSE7_EFW Dumps NSE7_EFW Practice Test NSE7_EFW Exam Questions