NSE7_EFW-7.0 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.0

Pass Fortinet NSE7_EFW-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_efw-7-0.html

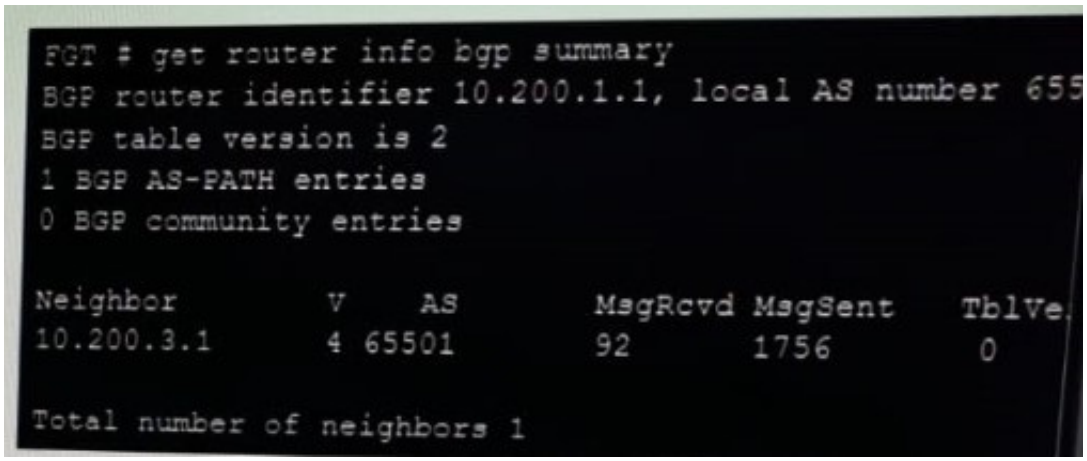
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to exhibit, which contains the output of a BGP debug command.



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.

Correct Answer: B

QUESTION 2

Examine the following partial outputs from two routing debug commands; then answer the question below.

get router info kernel

tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0

gwy=10.200.1.254 dev=2(port1)

tab=254 vf=0 scope=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0

gwy=10.200.2.254 dev=3(port2)

tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254

gwy=0.0.0.0 dev=4(port3)

get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3 dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is directly connected, port2

Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!

B. port2.

C. Both portl and port2.

D. port3.

Correct Answer: B

QUESTION 3

Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. FortiGate first checks the OSPF ID to elect a DR.

B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.

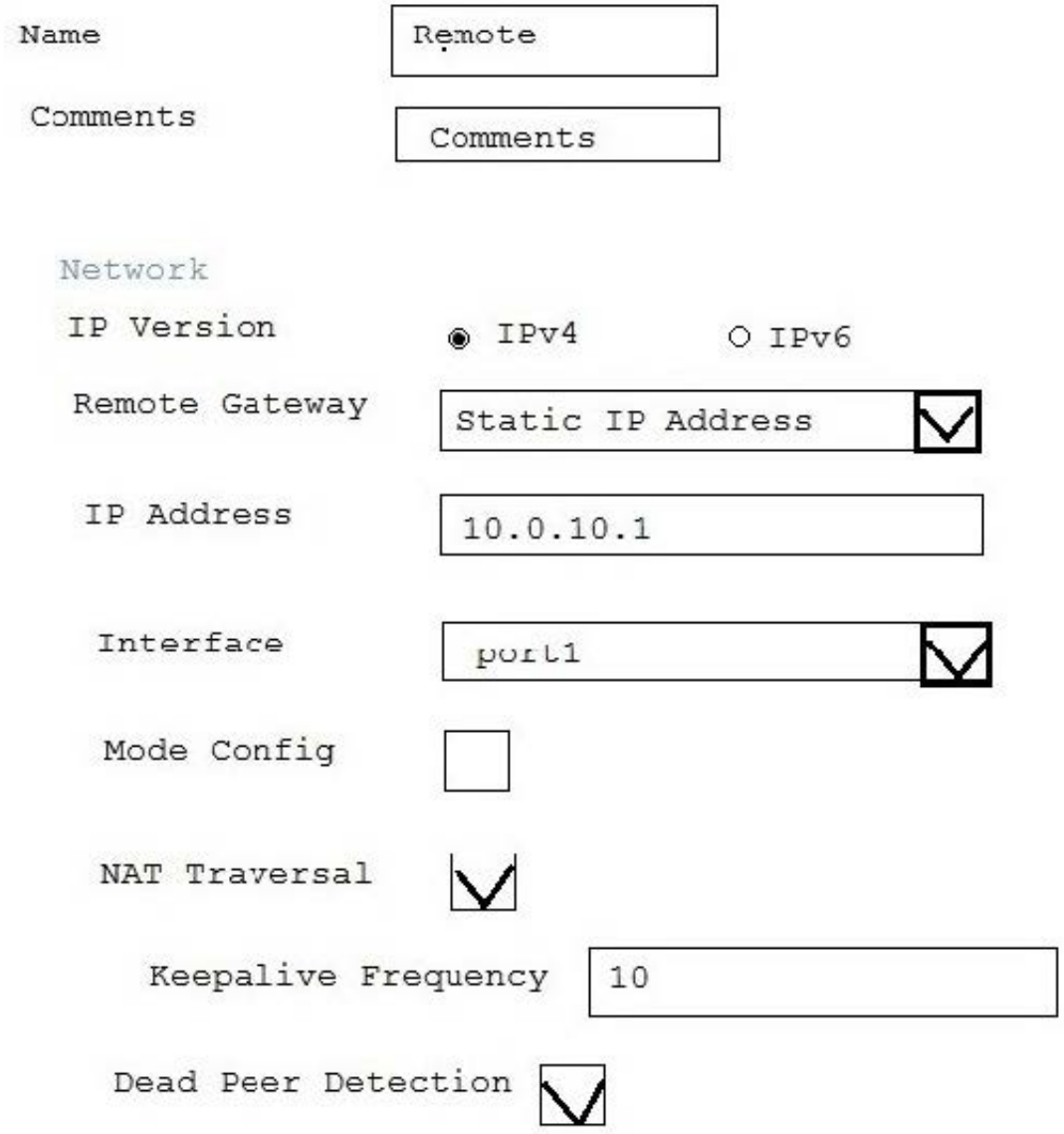
C. BDR is responsible for forwarding link state information from one router to another.

D. Only the DR receives link state information from non-DR routers.

Correct Answer: B

QUESTION 4

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

QUESTION 5

Refer to the exhibit, which shows the output of a debug command.

```
FGT # 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    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.

B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.

C. There are more than two OSPF routers on the wan2 network.

D. The interface ToRemote is a broadcast OSPF network.

Correct Answer: C

Explanation: Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

QUESTION 6

An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMSs in FortiManager. How should the administrator accomplish this task?

A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.

B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.

C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.

D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

Correct Answer: B

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 244

QUESTION 7

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

QUESTION 8

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

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

QUESTION 9

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 10

Refer to the exhibit, which shows the output of a diagnose command What can you conclude from the RTT value?

```
FGT # diagnose debug rating
Locale       : english
Service      : Web-filter
Status       : Enable
License      : Contract
Service      : Antispam
Status       : Disable
Service      : Virus Outbreak Prevention
Status       : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                  Weight  RTT    Flags   TZ   Packets   Curr Lost     Total Lost
64.26.151.37        10      45             -5   262432    0             846
64.26.151.35        10      46             -5   329072    0             6806
66.117.56.37        10      75             -5   71638     0             275
65.210.95.240       20      71             -8   36875     0             92
209.222.147.36      20      103     DI     -8   34784     0             1070
208.91.112.194      20      107     D      -8   35170     0             1533
96.45.33.65         60      144             0   33728     0             120
80.85.69.41         71      226             1   33797     0             192
62.209.40.74        150     97              9   33754     0             145
121.111.236.179     45      44      F      -5   26410     26226         26227
```

A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.

B. Its value is incremented with each packet lost.

C. It determines which FortiGuard server is used for license validation.

D. Its initial value is statically set to 10.

Correct Answer: A

QUESTION 11

Refer to the exhibit, which shows a session table entry.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=redir local may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

Which statement about FortiGate behavior relating to this session is true?

A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.

B. FortiGate forwarded this session without any inspection.

C. FortiGate is performing security profile inspection using the CPU. Most Voted

D. FortiGate applied only IPS inspection to this session.

Correct Answer: C

Explanation: Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 91, 92 First digit of "proto_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage

QUESTION 12

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

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

QUESTION 13

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 14

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: B

QUESTION 15

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

A. When run on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate device.

B. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

C. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.

D. When run on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate device.

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortimanager/6.2.1/administration- guide/71780/cli-scripts