NSE7^Q&As

Fortinet Troubleshooting Professional

Pass Fortinet NSE7 Exam with 100% Guarantee

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

https://www.passapply.com/nse7.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

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 2

When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.

B. The server requires more information from the user, such as the token code for two- factor authentication.

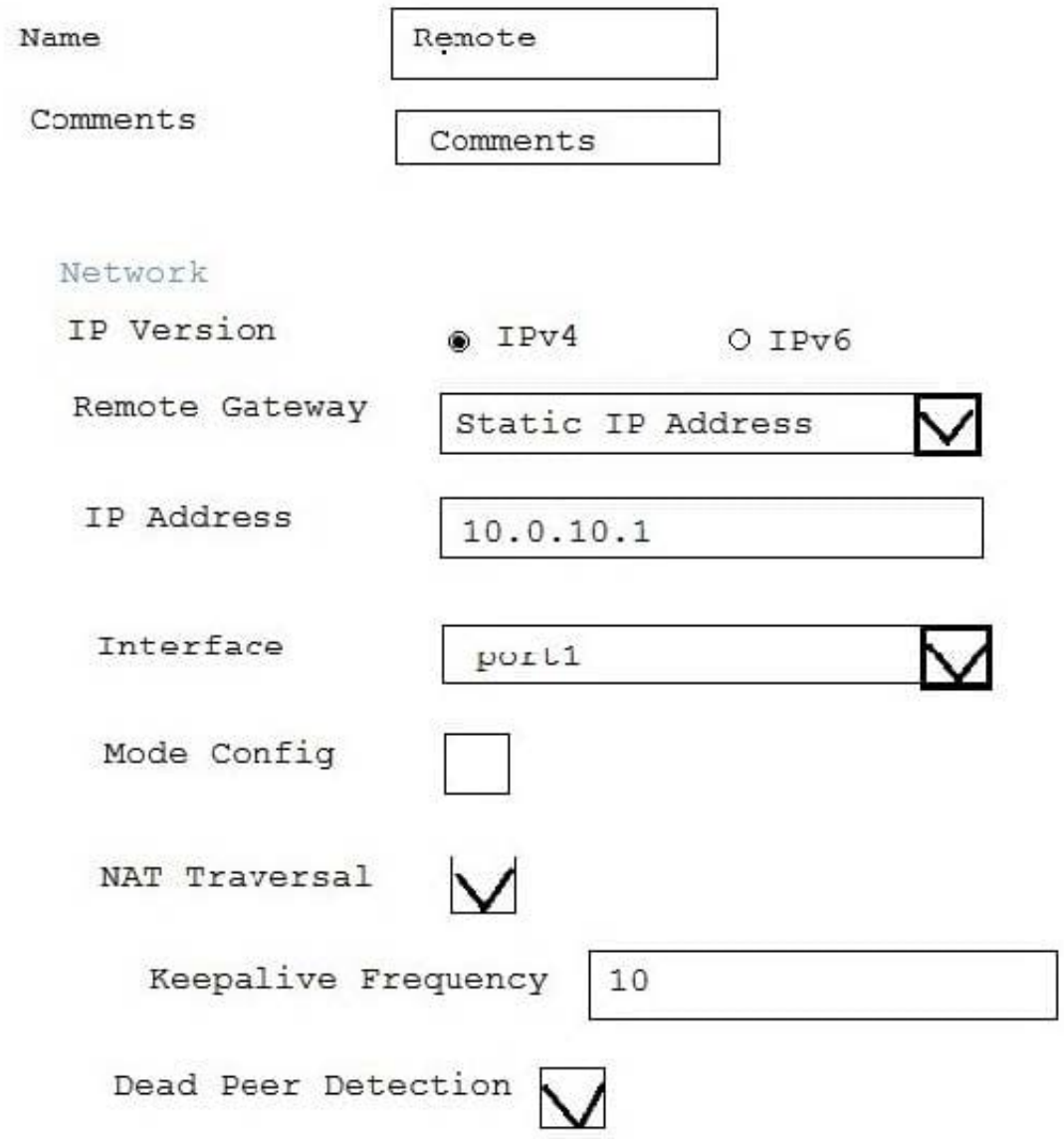
C. The user credentials are wrong.

D. The user account is not found in the server.

Correct Answer: B

QUESTION 3

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.

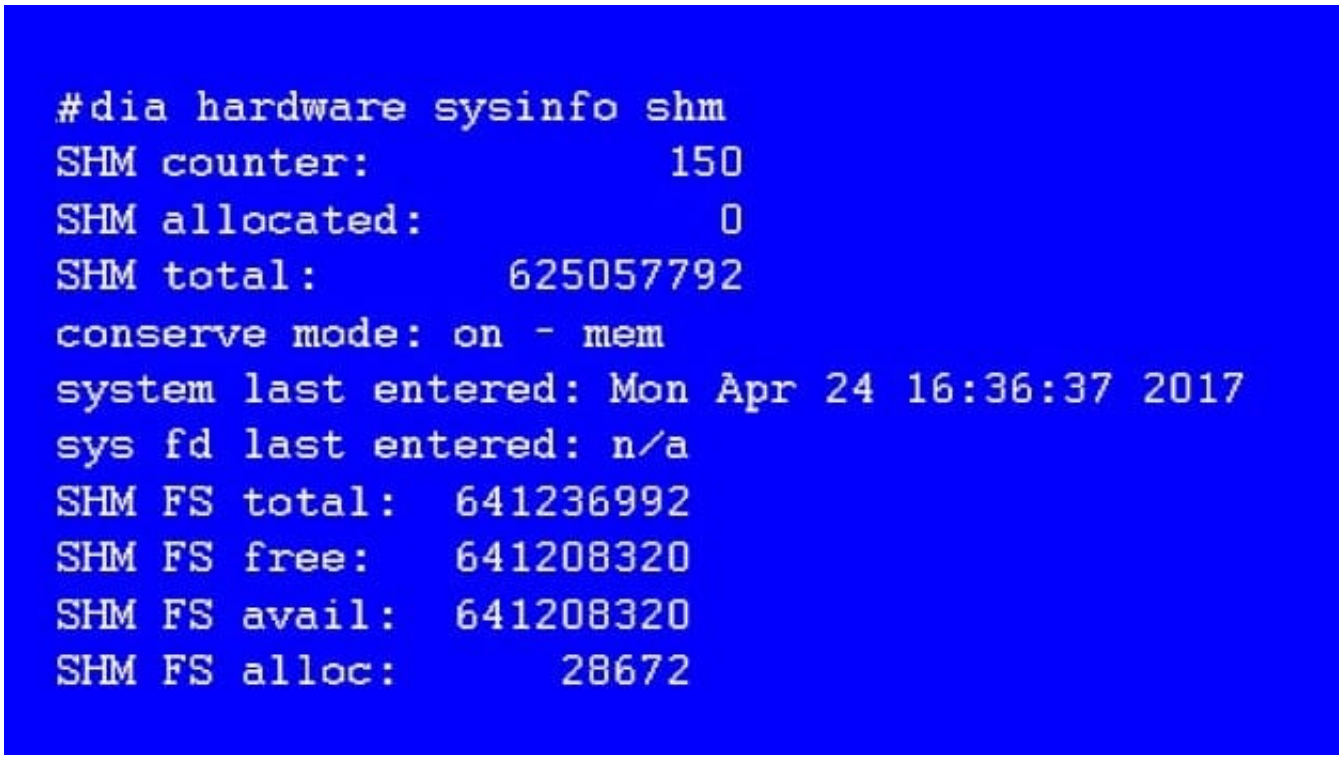
C. The IKE real time debug shows the phase 1 negotiation only. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.

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: A

QUESTION 4

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



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 5

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any `udp port 500\\'

B. diagnose sniffer packet any `udp port 4500\\'

C. diagnose sniffer packet any `esp\\'

D. diagnose sniffer packet any `udp port 500 or udp port 4500\\'

Correct Answer: C

QUESTION 6

Examine the output of the `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
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.

B. The TCP session for the BGP connection to 10.200.3.1 is down.

C. The local peer has received the BGP prefixed from the remote peer.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Correct Answer: B

QUESTION 7

An administrator has configured the following CLI script on FortiManager, which failed to apply any

changes to the managed device after being executed.

```
# conf rout stat
#     edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#     next
# end
```

Why didn\\'t the script make any changes to the managed device?

A. Commands that start with the # sign are not executed.

B. CLI scripts will add objects only if they are referenced by policies.

C. Incomplete commands are ignored in CLI scripts.

D. Static routes can only be added using TCL scripts.

Correct Answer: B

QUESTION 8

Which of the following statements are true about FortiManager when it is deployed as a local FDS? (Choose two.)

A. Caches available firmware updates for unmanaged devices.

B. Can be configured as an update server, or a rating server, but not both.

C. Supports rating requests from both managed and unmanaged devices.

D. Provides VM license validation services.

Correct Answer: AD

QUESTION 9

An administrator is running the following sniffer in a FortiGate:

diagnose sniffer packet any "host 10.0.2.10" 2

What information is included in the output of the sniffer? (Choose two.)

A. Ethernet headers.

B. IP payload.

C. IP headers.

D. Port names.

Correct Answer: BC

QUESTION 10

Which of the following statements are correct regarding application layer test commands? (Choose two.)

A. They are used to filter real-time debugs.

B. They display real-time application debugs.

C. Some of them display statistics and configuration information about a feature or process.

D. Some of them can be used to restart an application.

Correct Answer: BC

QUESTION 11

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 12

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

QUESTION 13

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
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)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
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
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 one of the following statements is true regarding FortiGate\\'s inspection of this session?

A. FortiGate applied proxy-based inspection.

B. FortiGate forwarded this session without any inspection.

C. FortiGate applied flow-based inspection.

D. FortiGate applied explicit proxy-based inspection.

Correct Answer: B

QUESTION 14

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

A. Primary unit stops sending HA heartbeat keepalives.

B. The FortiGuard license for the primary unit is updated.

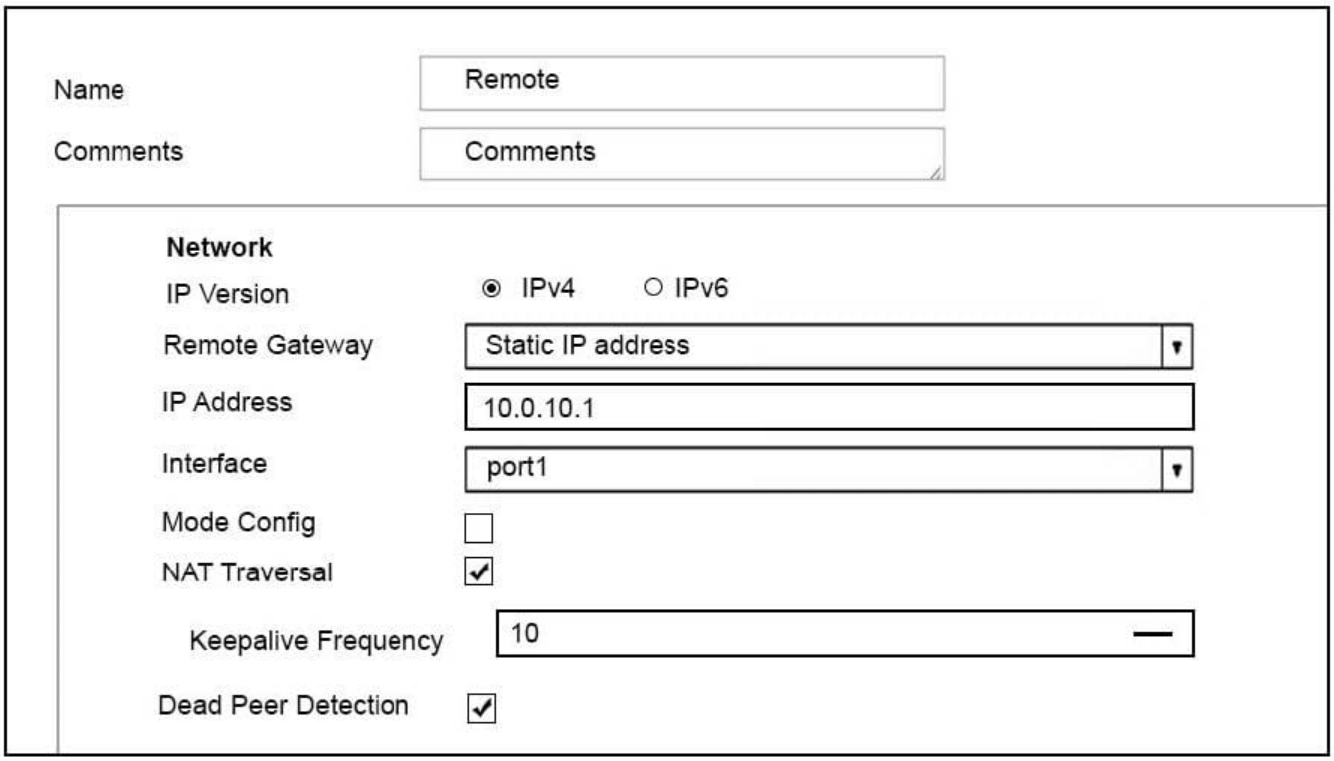
C. One of the monitored interfaces in the primary unit is disconnected.

D. A secondary unit is removed from the HA cluster.

Correct Answer: AB

QUESTION 15

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.



The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

A. The debug output shows phases 1 and 2 negotiations only. Once the tunnel is up, it does not show any more output.

B. The log-filter setting was set incorrectly. The VPN\\'s traffic does not match this filter.

C. The debug shows only error messages. If there is no output, then the tunnel is operating normally.

D. The debug output shows phase 1 negotiation only. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Correct Answer: D

NSE7 VCE Dumps NSE7 Practice Test NSE7 Braindumps