Fortinet NSE7_FSN_AR-7.6 NSE 7 Practice Questions

Shared by Waters on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Session entry

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 refresh_dir=both flags=00000000 socktype=0
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app_valid
statistic(bytes/packets/allow_err): org=1720/9/1 reply=10804/13/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->31/31->7 gwy=10.1.0.254/10.9.31.117
hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook=post dir=reply act=noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

The exhibit shows a session entry. Which statement about this TCP session is true?

Options:

A- The session will expire in one second.
B- It is a TCP session from 10.9.31.117 to 10.1.0.3.
C- The session is offloaded using NPU.
D- Return traffic to the initiator is sent to 10.9.31.117.

Answer:

C

Explanation:

The correct answer is C. The session is offloaded using NPU.

The exact session example in the study guide shows:

proto=6 this is a TCP session

expire=3599 the session will expire in 3599 seconds, not in one second

hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)

hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)

npu info: ... offload=8/8 ...

and the slide explicitly states: ''Offloaded in both directions using NP6''

The study guide also explains this exact point clearly:

''Counters for hardware acceleration---The presence of the npu info field indicates the session has been offloaded to hardware acceleration. In this example, traffic is being offloaded in both directions using network processor (NP) 6, which is represented by the value of 8.''

Why the other options are wrong:

A is wrong because expire=3599, not 1. The duration=1 field means the session has existed for 1 second, not that it will expire in 1 second.

B is wrong because the original session is from 10.9.31.117 to the remote server 200.8.57.5:443. The IP 10.1.0.3 is the SNAT-translated source address, not the final destination.

D is not the best answer for this single-select question. The reply is indeed DNATed back toward the original client, but the exact validated takeaway highlighted by the study guide for this exhibit is the NPU offload state.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

Diagnose output

```
# diagnose vpn tunnel list name 'VPN'
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=VPN ver=1 serial=8 172.16.50.251:4500->168.138.64.200:4500 tun_id=168.138.64.200 tun_id6=::168.138.64.200 dst_mtu=0 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/544 options[0220]=frag-rfc run_state=0 role=primary accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=6 ilast=59 olast=18 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=2 seqno=14
natt: mode=keepalive draft=32 interval=10 remote_port=4500
fec: egress=0 ingress=0
proxyid=VPN proto=0 sa=0 ref=1 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:0.0.0.0-255.255.255.255:0
run_tally=0
```

The output of the command diagnose vpn tunnels liar is shown.

Which two statements accurately describe the status of the tunnel? (Select two.)

Options:

A- Phase 2 is down
B- Phase 1 is down.
C- There is currently no traffic traversing the tunnel
D- Both Phase 1 and Phase 2 were negotiated successfully.

Answer:

A, C

Explanation:

Based on the Fortinet FCSS - Network Security 7.6 documents and the analysis of the VPN tunnel exhibit, here is the verified answer.

Questions no: 91

Verified Answer: A, C

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

To determine the status of the VPN tunnel, we must examine the specific counters and fields in the diagnose vpn tunnel list output provided in the exhibit.

Analyze Phase 2 Status (Option A):

The output displays child_num=0.

In IKEv2 (and IKEv1 implementations in FortiOS), 'Child SAs' refer to the Phase 2 (IPsec) Security Associations that carry the actual data traffic.

A value of 0 indicates that no Phase 2 tunnels are established. If Phase 2 were up, child_num would be at least 1.

Additionally, under the proxyid section, the field sa=0 confirms there is no active Security Association for that traffic selector.

Analyze Traffic Status (Option C):

The stat line shows: rxp=0 txp=0 rxb=0 txb=0.

rxp (Received Packets) and txp (Transmitted Packets) are both zero. This definitively confirms that no traffic is traversing the tunnel currently. This is expected since Phase 2 is down.

Analyze Phase 1 Status (Why B is incorrect):

The tunnel entry exists in the list with a valid tun_id, and NAT-Traversal is active (natt: mode=keepalive).

The presence of the tunnel in this command output, along with active Keepalive mechanisms, typically indicates that Phase 1 (IKE SA) is established and the peers are communicating on port 4500 (NAT-T), even though the data tunnels (Phase 2) failed to negotiate. If Phase 1 were down, the tunnel would often not appear in this 'list' view or would show different status flags indicating a complete connection failure.

Conclusion: The exhibit shows a scenario where the Phase 1 control channel is likely up (evidenced by the entry existence and NATT keepalives), but the Phase 2 data channel is down (child_num=0), resulting in zero traffic flow (rxp=0/txp=0).

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Output of `diagnose npu np6 port-list` on FortiGate 2000E

```
Chip    XAUI  Ports    Max    Cross-chip
                        Speed  offloading
------  ----  -------  -----  ----------
np6_1   0     port1    1G     No
        0     port5    1G     No
        0     port9    1G     No
        0     port13   1G     No
        0     port17   1G     No
        0     port21   1G     No

-omitted-
```

A partial output of diagnose npu up6 port-list on FortiGate 2000E is shown.

An administrator is unable to analyze traffic flowing between port1 and port17 using the diagnose sniffer command.

Which two commands allow the administrator to view the traffic? (Choose two.)

A)

```
diagnose npu np6 port-list disable 5 17
```

B)

```
config firewall policy
edit 5
set auto-asic-offload disable
end
next
edit 17
set auto-asic-offload disable
end
```

C)

```
diagnose npu np6 fastpath disable 1
```

D)

```
config system npu
set fastpath disable
end
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

B, C

Explanation:

The administrator cannot see traffic in the sniffer because it is being offloaded to the NPU (NP6). To view the traffic, offloading must be disabled so packets pass through the CPU.

B . config firewall policy ... set auto-asic-offload disable: This is the recommended method to troubleshoot specific traffic. By disabling ASIC offloading in the relevant firewall policies (Policies 5 and 17 in the exhibit), traffic is forced to the CPU and becomes visible to the sniffer.

C . diagnose npu np6 fastpath disable 1: This command temporarily disables the fastpath processing on the specific NP6 processor (ID 1) handling the ports. This forces all traffic handled by that NPU to the CPU, allowing the sniffer to capture it.

Incorrect Options: Option A uses invalid syntax (port-list disable is not a valid command). Option D (config system npu) is not the standard method for granular troubleshooting.

Question 4

Question Type: MultipleChoice

What are two reasons you might see iprope_in_check() check failed, drop when using the debug flow? (Select two.)

Options:

A- Packet was dropped because of policy route misconfiguration.
B- Packet was dropped because of traffic shaping.
C- Trusted host list misconfiguration.
D- VIP or IP pool misconfiguration.

Answer:

C, D

Explanation:

The Network Security Support Engineer 7.6 Study Guide explicitly explains this debug message:

''iprope_in_check() check failed, drop'' means the packet is destined to a FortiGate IP address and one of these conditions applies:

The service is not enabled

The service is using a different TCP port

The source IP address is not included in the trusted host list

The packet matches a local-in policy with action deny

That directly confirms C. Trusted host list misconfiguration.

Why D is the second valid choice:

The FortiOS administration guide explains that:

''IP pools and VIPs are considered local IP addresses if responding to ARP requests on these external IP addresses is enabled ... the FortiGate is considered a destination for those IP addresses ... once an IP pool or VIP has been configured ... the FortiGate considers it as a local address and will not forward traffic based on the routing table.''

Because iprope_in_check() is a local-in/local-destination type failure, a VIP or IP pool misconfiguration can cause traffic to be treated as destined for the FortiGate itself, which can then trigger this drop condition if the matching local service/local-in handling is not valid. So D is the closest supported second answer from the available choices.

Why the other options are wrong:

A is wrong because policy route problems are not the documented meaning of this specific debug message. The study guide instead ties iprope_in_check() check failed, drop to management/local-in conditions.

B is wrong because the study guide says traffic shaping drops appear as: ''Denied by quota check''

Question 5

Question Type: MultipleChoice

Which exchange lakes care of DoS protection in IKEv2?

Options:

A- Create_CHILD_SA
B- IKE_Auth
C- IKE_Req_INIT
D- IKE_SA_NIT

Answer:

C

Explanation:

TheIKE_SA_INITexchange in IKEv2 is responsible for DoS protection measures. During IKE_SA_INIT, before authentication and further exchange, the responder can use cookie challenges (per RFC 7296 and Fortinet VPN documentation). If a DoS attack is suspected (many

requests from the same source), the responder replies with a cookie. Only after the initiator returns the correct cookie does the exchange proceed, protecting the responder from state exhaustion and certain forms of DoS traffic at the handshake stage.

FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections

IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

Question 6

Question Type: MultipleChoice

Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.

Which action will FortiGate take when using the default settings for SSL certificate inspection?

Options:

A- FortiGate uses the SNI from the user's web browser.
B- FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
C- FortiGate uses the first entry listed in the SAN field in the server certificate.
D- FortiGate uses the CN information from the Subject field in the server certificate.

Answer:

D

Explanation:

When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, FortiGatedoes not block the connection; instead, it uses the CN value from the certificate's subject field to continue web filtering and categorization.

This behavior is described in the official Fortinet 7.6.4 Administration Guide:

''Check the SNI in the hello message with the CN or SAN field in the returned server certificate: Enable: If it is mismatched, use the CN in the server certificate.'' This is the default (Enable) mode, which differs from the Strict mode that would block the mismatched connection.

By default, this policy ensures service continuity and prevents disruptions due to certificate

mismatches, allowing FortiGate to log and inspect based on the CN even when the requested SNI does not match. It provides a balance between connection reliability and the accuracy of filtering by certificate identity, allowing security policies to remain functional without unnecessary blocks. This approach is recommended by Fortinet to maintain usability for end-users while still supporting granular inspection.

FortiGate 7.6.4 Administration Guide: Certificate Inspection

SSL/SSH Inspection Profile Configuration

Question 7

Question Type: MultipleChoice

Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 qwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=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=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
                             [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, port3
S           10.1.10.0/24 [10/0] via 10.1.0.1, port3
C           100.64.1.0/24 is directly connected, port1
C           100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

Options:

A- Set snat-route-change to enable.
B- Set the priority of the static default route using port2 to 1.
C- Set preserve-session-route to enable.
D- Set the priority of the static default route using port1 to 10.

Answer:

D

Explanation:

The 7.6 study guide explains the route selection order:

''Route Selection Process

Most specific route

Lowest distance

Lowest metric (dynamic routes)

Lowest priority (static routes)

ECMP (static, BGP, and OSPF routes)''**

It then states:

''If there are multiple routes with the same netmask, distance, metric, and priority, FortiGate shares the traffic among all of them. This is called equal-cost multi-path (ECMP).''

The FortiOS administration guide confirms the ECMP prerequisite:

''Routes must have the same destination and costs. In the case of static routes costs include distance and priority.''

In the exhibit, the kernel/FIB output shows the two default routes as:

gwy=100.64.1.254 dev=3 (port1) prio=0

gwy=100.64.2.254 dev=6 (port2) prio=10

So although both are default routes, their priorities are different. Since FortiGate uses the FIB/kernel for forwarding traffic, ECMP will not happen until the static-route priorities are the same. The study guide also notes that the FIB is the table used to perform standard routing

Therefore, to make the two default routes eligible for ECMP, the administrator must make the priorities equal. Since port2 is already 10, the needed change is to set the port1 default route priority to 10.

Why the other options are wrong:

A is wrong because snat-route-change affects how existing SNAT sessions react to routing changes, not whether static routes qualify for ECMP

B is wrong because changing port2 to priority 1 still would not match port1 at 0, so the routes still would not have equal cost for ECMP

C is wrong because preserve-session-route affects existing-session route persistence after routing changes, not ECMP qualification