



**Vendor:** Fortinet

**Exam Code:** FCSS\_NST\_SE-7.6

**Exam Name:** FCSS - Network Security 7.6 Support  
Engineer

**Version:** DEMO

### QUESTION 1

Refer to the exhibit. FortiGate is in conserve mode as shown in the Event logs.

Based on the information shown in the exhibit, what can you conclude about the FortiGate intrusion prevention system (IPS) configuration?

```
date=2024-05-06 time=14:14:29 logid="0100022700" type="event" subtype="system"
level="critical" vd="root" eventtime=1540790069 logdesc="IPS session scan paused"
action="drop" msg="IPS session scan, enter fail open mode"
```

- A. IPS fail open mode is disabled.
- B. The inspected protocol is not supported.
- C. The IPS profile is proxy based.
- D. New packets might pass through without inspection.

**Answer: D**

**Explanation:**

The “enter fail open mode” message tells you IPS is configured to fail-open under memory pressure, so new packets will be allowed through without full inspection when conserve mode kicks in.

### QUESTION 2

Refer to the exhibit, which shows the sniffer log on two FortiGate devices.

```
FGT-01
#diagnose sniffer packet any 'esp' 4
2024-03-07 15:57:40.344931 port1 out 42.123.56.38 -> 97.86.16.52: ESP spi=0xe8f9b3cf, seq=0x1e3415b)
2024-03-07 15:57:40.344949 port1 out 42.123.56.38 -> 97.86.16.52: ESP spi=0xe8f9b3cf, seq=0x1e3415c)
2024-03-07 15:57:40.344974 port1 out 42.123.56.38 -> 97.86.16.52: ESP spi=0xe8f9b3cf, seq=0x1e3415d)
2024-03-07 15:57:40.346832 port1 out 42.123.56.38 -> 97.86.16.52: ESP spi=0xe8f9b3cf, seq=0x1e3415e)
2024-03-07 15:57:40.347463 port1 out 42.123.56.38 -> 97.86.16.52: ESP spi=0xe8f9b3cf, seq=0x1e3415f)

FGT-02
#diagnose sniffer packet any 'esp' 4
(no packets captured)
```

The IPsec tunnel is up on both ends of the tunnel, but traffic is not flowing.

Based on the information in the log, which scenario explains the output on FortiGate FGT-02?

- A. The encryption method is not supported on FGT-02.
- B. A third-party device is blocking protocol 50.
- C. Hardware offload is disabled on FGT-02.
- D. The IKE daemon crashed.

**Answer: C**

**Explanation:**

No ESP packets show up on FGT-02's CPU because the tunnel traffic is being offloaded to its NP hardware, bypassing the kernel sniffer. In other words, hardware offload is active for IPsec on

FGT-02, so you won't see ESP in a CPU-based packet capture on that device.

### QUESTION 3

Which three conditions would prevent a static route from being used by the kernel to route traffic? (Choose three.)

- A. The interface specified in the route configuration is down.
- B. There is another route to the same destination, with a higher distance.
- C. The route has a lower metric than another route to the same destination.
- D. The next-hop IP address is unreachable and health monitor is configured.
- E. There is another route to the same destination, with a lower distance.

**Answer:** ADE

**Explanation:**

The interface specified in the route configuration is down.

If the egress interface is down (administratively or operationally), the kernel will mark the route inactive and won't use it.

The next-hop IP address is unreachable and health monitor is configured.

When a route's gateway fails its configured health check, the static route is suppressed until the monitor detects it as reachable again.

There is another route to the same destination, with a lower distance.

The kernel always prefers the route with the lowest administrative distance; any static route with a higher distance to an identical prefix is ignored.

### QUESTION 4

Refer to the exhibit, which shows a partial output of `diagnose npu np6 port-list` on FortiGate 2000E.

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

| Chip      | XAUI | Ports  | Max Speed | Cross-chip 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- |      |        |           |                       |

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. `config firewall policy`  
`edit 5`  
`set auto-asic-offload disable`  
`end`  
`next`  
`edit 17`  
`set auto-asic-offload disable`  
`end`
- B. `config system npu`  
`set fastpath disable`  
`end`
- C. `diagnose npu np6 port-list disable 5 17`
- D. `diagnose npu np6 fastpath disable 1`

**Answer:** CD

**Explanation:**

`diagnose npu np6 port-list disable 5 17`

This command disables hardware offloading for traffic on ports 5 (port1) and 17 (port17) of the NP6 processor, ensuring the CPU path is used so that diagnose sniffer can capture the packets.

`diagnose npu np6 fastpath disable 1`

Disabling the fastpath on NP6 chip 1 (np6\_1) forces all traffic through the regular processing path on that chip, which allows the sniffer to see the packets.

### QUESTION 5

Refer to the exhibit, which shows a partial output of the `fssod daemon real-time debug` command.

```
# diagnose debug application fssod -l
# diagnose debug enable
[fssod_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO
workstation=, ip=10.124.2.90 port=49215, time=1372061722
```

What two conclusions can you draw from the output? (Choose two.)

- A. Fortinet Single Sign-On (FSSO) is using DC Agent mode to detect logon events.
- B. FortiGate is frequently polling the workstation, in case the user has logged off.
- C. The collector agent cannot verify if the user is still logged in.
- D. FortiGate polled this event through TCP port 8000.
- E. FSSO is using agentless polling mode to detect logon events.

**Answer:** CE

**Explanation:**

The collector agent cannot verify if the user is still logged in.

In agentless-polling mode FSSO only reads Kerberos TGT events (e.g. 4768) from the DC's security log, and there's no corresponding "logoff" event - so it cannot confirm when a user logs off.

FSSO is using agentless polling mode to detect logon events.

The blank `workstation=` field and the use of event ID 4768 indicate that `fssod` is polling the domain controller's event log rather than receiving pushed events from a DC or collector agent.

### QUESTION 6

What are two reasons that an OSPF router does not have any type 5 link-state advertisements (LSAs) in its link-state database (LSDB)? (Choose two.)

- A. The local router is located in a stub area.
- B. IP protocol 89 is blocked between the local router and its peer.
- C. There is no autonomous system border router (ASBR) in the network.
- D. The peer of the local router is using a `prefix-list-out` configuration to prevent all type 5 LSAs to be advertised.

**Answer:** AC

**Explanation:**

The local router is located in a stub area.

Stub areas suppress Type 5 LSAs, so none appear in the LSDB.

There is no autonomous system border router (ASBR) in the network.

Without an ASBR there are no external routes to advertise, so no Type 5 LSAs are ever generated.

### QUESTION 7

Refer to the exhibit, which shows the partial output of `diagnose sys session stat`.

```
# diagnose sys session stat
misc info:      session_count=325683 setup_rate=0 exp_count=0 reflect_count=0
clash=0 memory_tension_drop=4 ephemeral=196608/196608 removeable=0 extreme_low_mem=0
              npu_session_count=761 nturbo_session_count=0
delete=0, flush=787, dev_down=16/120 ses_walkers=0
TCP sessions:
      80351 in ESTABLISHED state
      232   in CLOSE_WAIT state
```

An administrator has noticed unusual behavior from FortiGate. It appears that sessions are randomly removed.

Which two reasons could explain this? (Choose two.)

- A. The FortiGate is dropping all TCP sessions with incomplete three-way handshakes.
- B. The FortiGate is deleting sessions because the kernel cannot allocate more memory pages.
- C. The FortiGate is flushing sessions because of high memory usage.
- D. The FortiGate is not accepting sessions because the device has been down 16 out of 120 seconds.

**Answer:** BD

**Explanation:**

The FortiGate is deleting sessions because the kernel cannot allocate more memory pages. The `memory_tension_drop=4` counter shows that, under memory pressure, the oldest sessions are being removed when the system can't allocate new session blocks.

The FortiGate is not accepting sessions because the device has been down 16 out of 120 seconds.

The `dev_down=16/120` counter indicates 16 sessions were deleted due to an interface going down within the last 120 seconds.

## QUESTION 8

Refer to the exhibit, which contains the output of the command `diagnose vpn tunnel list`.

```
# 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 lqwy=static/1 tun=ntf 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
```

What is the status of the tunnel?

- A. Both Phase 1 and Phase 2 were negotiated successfully.
- B. Phase 2 is down.
- C. Traffic is passing through the tunnel.
- D. Phase 1 is down.

**Answer: B**

**Explanation:**

The key indicator is that `child_num=0` (and `sa=0` under the proxyid section), which means no IPsec child SAs (Phase 2 tunnels) are active - even though Phase 1 has been established, there are no Phase 2 SAs negotiated.

**QUESTION 9**

Which actions does FortiGate take after an administrator enables the auxiliary session setting? (Choose two.)

- A. FortiGate creates a new auxiliary session for each packet it receives.
- B. FortiGate only offloads auxiliary sessions.
- C. FortiGate creates two sessions in case of a routing change.
- D. FortiGate accelerates all ECMP traffic to the NP6 processor.

**Answer: CD**

**Explanation:**

FortiGate creates two sessions in case of a routing change.

When the return or incoming interface changes (for example due to ECMP or a routing update), FortiOS creates an auxiliary ("reflect") session alongside the original one, so that traffic can continue uninterrupted across both session paths.

FortiGate accelerates all ECMP traffic to the NP6 processor.

With auxiliary sessions enabled, even when traffic egresses/ingresses on different interfaces under ECMP, both the original and auxiliary sessions remain offloaded to the NP6, ensuring hardware acceleration is maintained.

**QUESTION 10**

Refer to the exhibit, which contains a screenshot of some phase 1 settings.

## VPN partial configuration

|                     |                           |
|---------------------|---------------------------|
| Name                | Remote                    |
| Comments            | Comments 0/255            |
| <b>Network</b>      |                           |
| IP Version          | IPv4 IPv6                 |
| Remote Gateway      | Static IP Address         |
| IP Address          | 10.0.10.1                 |
| Interface           | port1                     |
| Local Gateway       | <input type="checkbox"/>  |
| Mode Config         | <input type="checkbox"/>  |
| NAT Traversal       | Enable Disable Forced     |
| Keepalive Frequency | 10                        |
| Dead Peer Detection | Disable On Idle On Demand |

The VPN is up. To monitor traffic flow, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose sniffer packet any 'udp and port 500' 4
diagnose debug enable
```

However, the sniffer does not show any output. Why?

- A. Change the filter to sniff protocol TCP.
- B. It must sniff IP address 10.0.10.1.
- C. Change the filter to sniff traffic on port1.
- D. NAT Traversal is enabled.

**Answer: D**

**Explanation:**

With NAT-T on, IKE traffic is encapsulated in UDP port 4500 (not port 500) once the tunnel is up, so your `udp port 500` filter never matches any packets.

## 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
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/100.0.0.2
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(192.167.11.100:49545)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
src mac=08:5b:0e: 6c:76:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 to=ff/ff app_list=0 app=0 url_cat=41
rpd_b_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 correct?

- 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 a security profile inspection using the CPU.
- D. FortiGate applied only IPS inspection to this session.

**Answer: A**

**Explanation:**

The key here is the `state=redir_local...auth` flag, which tells that this session is being locally redirected (i.e. captive-portal) waiting for the user to authenticate before it will match the “real” policy.

## QUESTION 22

Which exchanges are the first two exchanges in IKEv2 negotiation?

- A. INIT\_Req and Auth\_Request
- B. IKE\_SA\_INIT and IKE\_Auth
- C. Key Exchange and Authentication
- D. Init\_Req and Wait\_Init\_Req

**Answer: B**

**Explanation:**

The first IKEv2 exchange is the SA\_INIT, where algorithms, nonces, and Diffie-Hellman values are negotiated. The second is the AUTH exchange, which carries peer authentication and completes the IKE SA setup.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**