Vendor: Fortinet

Exam Code: FCSS_NST_SE-7.4

Exam Name: FCSS - Network Security 7.4 Support Engineer

Version: DEMO

QUESTION 1
Refer to the exhibit, which shows the partial output of `diagnose sys session stat`.

```
# diagnose sys  session stat
misc info:     session_count=1523 setup_rate=0 exp_count=0 reflect_count=0 clash=113
   memory_tension_drop=0 ephemeral=0/131072 removeable=0 extreme_low_mem=0
   npu_session_count=0
delete=0, flush=1, dev_down=0/0
session walkers: active=0, vf-42, dev-0, saddr-0, npu-0
TCP sessions:
    562 in ESTABLISHED state
    15 in SYN_RECV state
    27 in CLOSE state
```

Which statement about the output shown in the exhibit is correct?

A. 27 sessions have expired but are still in the session table in case any out-of-order packets arrive.
B. 15 sessions have been categorized as ephemeral.
C. 113 sessions have been dropped because of memory page exhaustion.
D. 562 TCP sessions have their `proto_state` set to `01` if there is no inspection.

Answer: D
Explanation:
The 562 sessions shown as “in ESTABLISHED state” correspond to proto_state 01 when no deeper inspection is applied.

QUESTION 2
Which of the following regarding protocol states is true?

A. `proto_state=10` indicates an established TCP session.
B. `proto_state=00` indicates that UDP traffic flows in both directions.
C. `proto_state=01` indicates one-way ICMP traffic.
D. `proto_state=01` indicates an established TCP session.

Answer: D
Explanation:
The `proto_state` field is actually a two-bit bitmask where the bits track seen packet directions, but for TCP FortiGate only flips into `01` once the three-way handshake completes and the session is fully established. UDP sessions never set those bits (they stay at `00`), and ICMP uses its own state machine. Seeing `proto_state=01` in a TCP session listing always means that the TCP handshake has finished and the session is established.

QUESTION 3
Refer to the exhibit. Antivirus is unable to detect an infected file downloaded through HTTPS. Part of the configuration used for antivirus inspection is shown in the exhibit.

Which configuration changes can be performed to inspect HTTPS?

Antivirus profile configuration

```
config antivirus profile
    edit "Block"
        config http
            set av-scan block
        end
        config ftp
            set av-scan block
        end
        config imap
            set av-scan block
        end
        config pop3
            set av-scan block
        end
        config smtp
            set av-scan block
        end
    next
end
```

Firewall policy configuration

```
config firewall ssl-ssh-profile
edit "certificate-inspection"
        set comment "SSL handshake inspection."
        config https
            set ports 443
            set status certificate-inspection
            set quic inspect
        end
        config ftps
            set status disable
        end
        config imaps
            set status disable
        end
        config pop3s
            set status disable
        end
        config smtps
            set status disable
        end
        config ssh
            set ports 22
            set status disable
        end
        config dot
            set status disable
            set quic inspect
            set unsupported-ssl-version allow
        end
    next
end
```

A. Set a different antivirus database.
B. Increase the maximum number of subdirectories and nested archives.
C. Disable the `emulator` setting.
D. Enable SSL deep inspection.

Answer: D
Explanation:
You must switch from mere certificate inspection to full SSL deep inspection on the HTTPS profile so that the FortiGate can decrypt the traffic and pass it through the AV engine. In practice this means editing the SSL/SSH profile and setting the HTTPS inspection mode to deep-inspection (and ensuring your CA cert is installed on the clients).

QUESTION 4
Refer to the exhibit, which shows the output of a BGP debug command.

```
# get router info bgp summary

VRF 0 BGP router identifier 172.16.23.58, local AS number 65100
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
172.16.23.153   4        100     218     3220        0    0    0 never     Connect

Total number of neighbors 1
```

Why has the local router at 172.16.23.58 been unable to establish adjacency with its only neighbor?

A. The local router has not received a `keepalive` message from the neighbor.
B. There is no active route to the BGP neighbor.
C. The local router has not received a `SYN/ACK` packet from the neighbor.
D. The local router has not received an `OPEN` message from the neighbor.

Answer: C
Explanation:
In BGP's Connect state the router has sent the initial TCP SYN but hasn't received the SYN/ACK from its peer, so the TCP handshake never completes and adjacency can't form.

QUESTION 5
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 6
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 7
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 8
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 9
Refer to the exhibit, which shows a partial output of the `fssod daemon real-time debug` command.

```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_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.

Thank You for Trying Our Product

Braindump2go 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.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14