Vendor: Fortinet

Exam Code: NSE7_NST-7.2

Exam Name: Fortinet NSE 7 - Network Security 7.2 Support Engineer

Version: DEMO

QUESTION 1
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: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
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 forwarded this session without any inspection.
B. FortiGate is performing a security profile inspection using the CPU.
C. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
D. FortiGate applied only IPS inspection to this session.

Answer: B
Explanation:
The session table entry provided shows detailed information about a specific network session passing through the FortiGate device. From the session details, we can see that the session has various attributes such as state, protocol, policy, and inspection details.

The session state (proto_state=11) indicates that the session is being actively processed and inspected.

The npd_state=00000000 suggests that the session is being handled by the CPU rather than offloaded to a Network Processor (NP).

The session is marked for security profile inspection, evident from the detailed byte/packet counts and other session parameters.

From these indicators, it's clear that FortiGate is using its CPU to perform security profile inspection on this session rather than simply forwarding the traffic without inspection or relying solely on IPS inspection.

QUESTION 2
What is the diagnose test application ipsmonitor 5 command used for?

A. To disable the IPS engine
B. To provide information regarding IPS sessions

C. To restart all IPS engines and monitors
D. To enable IPS bypass mode

Answer: C
Explanation:
The command diagnose test application ipsmonitor 5 is used to restart all IPS (Intrusion Prevention System) engines and monitors on the FortiGate device. This command is part of the diagnostic tools available for troubleshooting and maintaining the IPS functionality on the FortiGate.

Running this command forces the IPS system to reset and reinitialize, which can be useful in situations where the IPS functionality appears to be malfunctioning or not responding correctly.

This action helps in clearing any issues that might have arisen due to internal errors or misconfigurations, ensuring that the IPS engines operate correctly after the restart.

QUESTION 3
Refer to the exhibit, which shows the modified output of the routing kernel.

```
get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Which statement is true?

A. The BGP route to 10.0.4.0/24 is not in the forwarding information base.
B. The default static route through port2 is in the forwarding information base.
C. The default static route through 10.200.1.254 is not in the forwarding information base.
D. The egress interface associated with static route 8.8.8.8/32 is administratively up.

Answer: B
Explanation:
The routing table shown in the exhibit lists all the routes known to the FortiGate device. It includes routes learned through different protocols such as BGP, OSPF, and static routes.

The entry S * 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0] indicates that there is a static route to the default gateway (0.0.0.0/0) through port2 with a gateway IP of 10.200.2.254.

The asterisk * next to the route signifies that this route is selected and currently active in the forwarding information base (FIB). This means the FortiGate uses this route to forward packets destined for addresses not otherwise specified in the routing table.

QUESTION 4
Refer to the exhibit. If the default settings are in place, what can you conclude about the conserve mode shown in the exhibit?

```
# diagnose hardware sysinfo conserve
memory conserve mode:              on
total RAM:                         3040 MB
memory used:                       2706 MB 89% of total RAM
Memory freeable:                    334 MB 11% of total RAM
memory used + freeable threshold extreme:  2887 MB 95% of total RAM
memory used threshold red:         2675 MB 88% of total RAM
memory used threshold green:       2492 MB 82% of total RAM
```

A. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
B. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings because of high memory use.
C. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Answer: A
Explanation:
Conserve Mode Overview: Conserve mode is a state that FortiGate enters to protect itself from running out of memory. It is triggered when the memory usage reaches certain thresholds.

Thresholds: The default settings for conserve mode thresholds are:

Red Threshold: 88% memory usage.

Extreme Threshold: 95% memory usage.

Green Threshold: 82% memory usage.

Impact on Sessions: When in conserve mode:

New sessions requiring flow-based content inspection are blocked.

New sessions requiring proxy-based content inspection are also blocked to free up memory resources.

Current Memory State in Exhibit: The exhibit shows:

Total RAM: 3040 MB.

Memory used: 2706 MB (89% of total RAM).

Memory usage exceeds the red threshold (88%), thus triggering conserve mode.

Given that the memory usage is above the red threshold and conserve mode is active, the FortiGate will block new sessions requiring both flow-based and proxy-based content inspection to conserve memory.

QUESTION 5
Refer to the exhibit, which shows the output of get router info bgp neighbors 100.64.2.254.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1            xxx       0        0          100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP state of the two BGP participants is OpenConfirm.
D. The local router is adverting the 10.20.30.40/24 network to its BGP neighbor.

Answer: D
Explanation:
BGP Advertisement: The output from the command get router info bgp neighbors 100.64.2.254 advertised-routes shows the routes that the local router is advertising to its BGP neighbor.

Output Analysis:

The Network column lists the networks being advertised.

The Next Hop column indicates the next-hop IP address for these routes.

The line *> 10.20.30.40/24 100.64.2.1 indicates that the 10.20.30.40/24 network is being advertised with a next-hop of 100.64.2.1.

Local Router's Role: Since the output lists the advertised routes, it means that the local router (with router ID 172.16.1.254) is advertising the 10.20.30.40/24 network to its neighbor 100.64.2.254.

This confirms that the local router is indeed advertising the specified network to its BGP neighbor.

QUESTION 6
Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

A. Refused connection. Potential mismatch of TCP port.
B. Mismatched pre-shared password.
C. Inability to reach IP address of the collector agent.
D. Log is full on the collector agent.
E. Incompatible collector agent software version.

Answer: ABC
Explanation:
Refused Connection: A refused connection typically indicates a mismatch in the TCP port configuration between the FortiGate and the collector agent. Ensuring both are configured to use the same TCP port is crucial for proper connectivity.

Mismatched Pre-Shared Password: If the pre-shared password configured on the FortiGate does not match the one set on the collector agent, authentication will fail, leading to connectivity issues.

Inability to Reach IP Address: This can occur due to network issues such as incorrect routing, firewall rules blocking traffic, or the collector agent being down. Verifying network connectivity and the status of the collector agent is necessary to resolve this issue.

QUESTION 7
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. FSSO is using agentless polling mode to detect logon events.
B. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on
C. The logon event can be seen on the collector agent installed on Windows.
D. FSSO is using DC agent mode to detect logon events.

Answer: CD
Explanation:
Logon Event on Collector Agent: The debug output indicates that the logon event is recorded, showing that the collector agent on Windows is logging user activities and transmitting this data to the FortiGate.

DC Agent Mode: The presence of detailed logon events and their corresponding metadata, such as the domain and workstation information, suggests that the FortiGate is using DC agent mode. This mode involves an agent installed on the Domain Controller (DC) to capture and forward logon events.

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

10% Discount Coupon Code: **ASTR14**