Number: NSE7_NST-7.2
Passing Score: 800
Time Limit: 120
File Version: 2.2

Exam Code: NSE7_NST-7.2

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

Exam A

QUESTION 1
Refer to the exhibit.

```
# 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
```

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

Correct Answer: C, D
Section:
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.
Fortinet Community: How FSSO Works and Troubleshooting Steps (Welcome to the Fortinet Community!) (Fortinet GURU).

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

Correct Answer: C
Section:
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
There are four exchanges during IKEv2 negotiation.
Which sequence is correct?

A. IKE_Proposal, ID_Auth, PiggyBack_CHILD and Informational

B. lnit_Req, Wait_lnit_Req, ID_Auth_Req and Create_CHILD_SA
C. INIT_Re, INIT_Auth, ID_Child and SET_Nonce
D. IKE_SAJNIT, IKE_Auth, Create_CHILD_SA and Informational

Correct Answer: D
Section:
Explanation:
IKE_SA_INIT:
This is the first exchange in IKEv2. It establishes a secure, authenticated channel between peers and negotiates cryptographic algorithms and keys.
IKE_Auth:
The second exchange authenticates the IKE SA (Security Association) using the previously negotiated keys and algorithms. This exchange also establishes the first IPsec SA.
Create_CHILD_SA:
This exchange creates additional IPsec SAs after the initial authentication. It can also be used to rekey existing IPsec SAs to maintain security.
Informational:
This is a generic exchange used for various purposes such as error notification, deletion of SAs, and other control messages.
Fortinet Community: IKEv2 packet exchanges and troubleshooting
Fortinet Documentation: IPsec VPN Concepts

QUESTION 4
Exhibit.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/if ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

Refer to the exhibit, which shows the output of diagnose sys session list.
If the HA ID for the primary device is 0. what happens if the primary fails and the secondary becomes the primary?

A. The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.
B. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.
C. Traffic for this session continues to be permitted on the new primary device after failover. without requiring the client to restart the session with the server.
D. The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.

Correct Answer: C
Section:
Explanation:
Session Synchronization:
FortiGate HA (High Availability) ensures that active sessions are synchronized between the primary and secondary devices. This synchronization allows for seamless failover and continuity of sessions.

Handling NAT Sessions:
The session in the exhibit has NAT applied, as indicated by the hook=post dir=org act=snat entry. FortiGate's HA setup is designed to handle such sessions, ensuring that traffic continues without interruption during failover.
Session Preservation:
Even with the presence of NAT, the session state is preserved across the HA devices. This means that ongoing sessions do not require re-establishment by the client, thus providing a seamless experience.
Fortinet Documentation: HA session synchronization and failover
Fortinet Community: Understanding session synchronization in FortiGate HA

QUESTION 5
Refer to the exhibit, which shows the omitted output of FortiOS kernel slabs.

```
…
packet_de_duplication     0      0    128    30    1 : tunables  252  126    0 : slabdata      0      0      0
ip6_nat_record            0      0    128    30    1 : tunables  252  126    0 : slabdata      0      0      0
tcp6_session              0      0   1536     5    2 : tunables   60   30    0 : slabdata      0      0      0
ip6_session               0      0   1300     3    1 : tunables   60   30    0 : slabdata      0      0      0
ip_nat_record             0      0     64    59    1 : tunables  252  126    0 : slabdata      0      0      0
sctp_session              0      0   1600     5    2 : tunables   60   30    0 : slabdata      0      0      0
tcp_session               3      5   1500     5    2 : tunables   60   30    0 : slabdata      1      1      0
ip_session                1      3   1200     3    1 : tunables   60   30    0 : slabdata      1      1      0
…
```

Which statement is true?

A. The total slab size of the tcp_sessior. slab Is 7500 kB and is associated with the kernel.
B. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
C. The total slab size of the sctp_session slab is 0 kB and is associated with the user space
D. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.

Correct Answer: B
Section:
Explanation:
Kernel Slabs Overview:
The slab allocator in the Linux kernel is used for efficient memory management. It groups objects of the same type into caches, which are divided into slabs.
Each slab contains multiple objects and helps to minimize fragmentation and enhance memory allocation efficiency.
Interpreting the Exhibit:
The exhibit shows output related to various kernel slab caches.
The line for ip6_session indicates that there are 1300 kB allocated for this slab, which means the total memory size allocated for IPv6 session objects in the kernel is 1300 kB.
Fortinet Community: Explanation of kernel slab allocation and usage (Welcome to the Fortinet Community!) (Hammertux).
Linux Kernel Documentation: Slab Allocator details (Hammertux).

QUESTION 6
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?

A. FortiGate closes the connection because this represents an invalid SSL/TLS configuration
B. FortiGate uses the 31 information from the Subject field in the server certificate.
C. FortiGate uses the first entry listed in the SAN field in the server certificate.
D. FortiGate uses the SNI from the user's web browser.

Correct Answer: A
Section:
Explanation:

SNI and Certificate Mismatch: When 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, FortiGate's default behavior is to consider this as an invalid SSL/TLS configuration.
Default Action: FortiGate, under default settings for SSL certificate inspection, will close the connection to prevent potential security risks associated with mismatched certificates.
Fortinet Community: SSL Certificate Inspection Configuration and Behavior (Welcome to the Fortinet Community!).

QUESTION 7
Exhibit.

```
Hub # get vpn ipsec tunnel details
gateway
    name: 'Hub2Spoke1'
    type: route-based
    local-gatewav: 10.10.1.1:0 (static)
    remote-gateway: 10.10.2.2:0 (static)
    mode: ike-vl
    interface: 'wan2' (6)
    rx packets: 1025 bytes: 524402 errors: 0
    tx packets: 641 bytes: 93 errors: 0
    dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
    selectors
      name: 'Hub2Spoke1'
      auto-negotiate: disable
      mode: tunnel
      src: 0:192.168.1.0/0.0.0.0:0
      dst:0:10.10.20.0/0.0.0.0:0
      SA
        lifetime/rekey: 43200/32137
        mtu: 1438
        tx-esp-seq: 2ce
        replay: enabled
      inbound
        spi: 01e54b14
        enc: aes-cb 914dc5d092667ed436ea7f6efb867976
        auth:  shal a81b019d4cdfda32ce51e6b01d0blea42a74adce
      outbound
        spi: 3dd3545f
        enc:  aes-cb 017b8ff6c4ba2leac99b22380b7de74d
        auth: shal   edd8141f4956140eef703d9042621d3dbf5cd961
      NPU acceleration: encryption (outbound) decryption (inbound)
```

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command. Based on the output, which two statements are correct? (Choose two.)

A. Anti-replay is enabled.
B. The npu_flag for this tunnel is 03.
C. The npu_flag for this tunnel is 02
D. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.

Correct Answer: A, C
Section:
Explanation:
Anti-replay Enabled:
The exhibit shows replay: enabled, which confirms that anti-replay is enabled for this IPsec tunnel. Anti-replay is a security feature that prevents replay attacks by ensuring that packets are not duplicated or reused.
NPU Acceleration:
The NPU acceleration: encryption (outbound) decryption (inbound) line indicates that Network Processing Unit (NPU) acceleration is used.
The npu_flag for this tunnel is 02. This indicates that encryption and decryption are handled by the NPU, improving the performance of the VPN tunnel.

Fortinet Community: Troubleshooting IPsec VPN Tunnels (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).
Fortinet Documentation: Verifying IPsec VPN Tunnels (Fortinet Docs) (Fortinet Docs).

QUESTION 8
Which two statements about conserve mode are true? (Choose two.)

A. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.
B. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
D. FortiGate exits conserve mode when the system memory goes below the configured green threshold

Correct Answer: A, D
Section:
Explanation:
Conserve Mode Activation:
FortiGate enters conserve mode to prevent system crashes when the memory usage reaches critical levels. The 'red threshold' is the point at which FortiGate starts dropping new sessions to conserve memory.
When the system memory usage exceeds this threshold, the FortiGate will block new sessions that require significant memory resources, such as those needing content inspection.
Exiting Conserve Mode:
The 'green threshold' is the memory usage level below which FortiGate exits conserve mode and resumes normal operation.
Once the system memory usage drops below this threshold, FortiGate will start allowing new sessions again.
Fortinet Community: Understanding conserve mode and its thresholds (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).
Fortinet Documentation: Memory conserve mode and thresholds (Welcome to the Fortinet Community!) (Fortinet GURU).

QUESTION 9
Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.
If the priority on route ID _ were changed from 10 to 0, what would happen to traffic matching that user session?

A. The session would be deleted, and the client would need to start a new session.
B. The session would remain in the session table, but its traffic would now egress from both port1. andport2.
C. The session would remain in the session table, and its traffic would egress from port2.
D. The session would remain in the session table, and its traffic would egress from port1.

Correct Answer: C
Section:
Explanation:
The exhibits show the configuration of static routes and a session table entry for an active session. The static routes are configured with different priorities:
Route through port1 with a gateway of 10.200.1.254 and priority 5.
Route through port2 with a gateway of 10.200.2.254 and priority 10.
If the priority of the route through port2 is changed from 10 to 0, this route will become more preferred than the route through port1 because lower priority values indicate higher preference. As a result, the traffic for the existing session will switch to using the more preferred route:
The session would remain active in the session table, as FortiGate does not immediately clear sessions upon route changes unless explicitly configured to do so.
The traffic for the session would then start egressing from port2, which now has the higher priority route due to its lower priority value.
Fortinet Documentation on Routing Configuration
Fortinet Community on Session Handling

QUESTION 10
Refer to the exhibit, which shows oneway communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)

A. Ensure the port for Neighbor Discovery has been changed.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way
D. You must authorize the downstream FortiGate on the root FortiGate.
E. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.

Correct Answer: C, D, E
Section:
Explanation:
The exhibit shows a sniffer capture where TCP port 8013 is being used for communication. The communication appears one-way, indicating potential issues with the upstream FortiGate receiving the necessary packets or being able to respond.
To ensure successful communication in a Security Fabric setup:
Ensure TCP port 8013 is not blocked along the way: Verify that no firewalls or network devices between the downstream and upstream FortiGates are blocking TCP port 8013. This port is crucial for Security Fabric communication.
Authorize the downstream FortiGate on the root FortiGate: In the Security Fabric, the root FortiGate must recognize and authorize the downstream FortiGate to allow proper communication and management.
Enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate: The upstream FortiGate must have the Security Fabric or Fortitelemetry enabled on the interface that receives the communication from the downstream FortiGate. This enables proper data exchange and monitoring within the Security Fabric.
Fortinet Documentation on Security Fabric Configuration
Fortinet Community Discussion on Port Requirements

QUESTION 11
Refer to the exhibit, which shows the output of a BGP debug command.

```
# get router info bgp summary

VRF 0 BGP router identifier 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      1756       0       0    0  never    Connect

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router initiated the BGP session to 10.200.3.1 but did not receive a response.

B. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConf inn yet.
C. The router 10.200.3.1 has authentication configured for BGP and the local router does not.
D. The local router has a different AS number than the remote peer.

Correct Answer: A
Section:
Explanation:
The BGP summary output shows the state of the 10.200.3.1 peer as 'Connect.' This state indicates that the local router has attempted to initiate a BGP session with the peer, but the peer has not yet responded to the initial connection request.
State Explanation: The 'Connect' state in BGP indicates that the TCP connection has been initiated but is waiting for a response. If the peer does not respond within the configured timers, the session will transition to the 'Active' state and retry the connection.
Possible Causes: This can occur due to network issues preventing the peer from responding, a misconfiguration on the peer device, or issues like access control lists (ACLs) blocking the BGP traffic.
To troubleshoot, check the connectivity between the routers, ensure that the BGP configurations on both sides match, and verify that there are no firewalls or ACLs blocking the BGP packets.
Fortinet Documentation on BGP Troubleshooting
Fortinet Community Discussion on BGP State Issues

QUESTION 12
Refer to the exhibit, which shows two entries that were generated in the FSSO collector agent logs.

```
… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
… failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

What three conclusions can you draw from these log entries? (Choose three.)

A. Remote registry is not running on the workstation.
B. The FortiGate firmware version is not compatible with that of the collector agent
C. DNS resolution is unable to resolve the workstation name.
D. The user's status shows as 'not verified' in the collector agent
E. A firewall is blocking traffic to port 139 and 445.

Correct Answer: A, C, E
Section:
Explanation:
The exhibit shows log entries from the FSSO (Fortinet Single Sign-On) collector agent logs. These logs provide insights into why there might be issues with the collector agent connecting to workstations or the registry.
Remote registry is not running on the workstation: The failure to connect to the workstation registry can occur if the remote registry service on the workstation is not running. This service needs to be active to allow the FSSO collector agent to query the workstation for user login information.
DNS resolution is unable to resolve the workstation name: The logs indicate a failure in connecting to a workstation by name, which can happen if the DNS server is unable to resolve the workstation's name to an IP address. This is a common issue when the DNS settings are incorrect or the workstation name is not properly registered in the DNS.
A firewall is blocking traffic to port 139 and 445: Communication issues to the workstation or registry are often caused by firewall rules blocking essential ports. Ports 139 (NetBIOS) and 445 (SMB) are critical for these operations. Ensure these ports are open on both the workstation and any intermediate firewalls.
Fortinet Community Documentation on FSSO Troubleshooting
Fortinet Community on FSSO Collector Agent Issues

QUESTION 13
Refer to the exhibit, which shows the output of a real-time debug.

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training. fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9 (ftgd-allow) wf-act=5 (ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which statement about this output is true?

A. The server hostname was extracted from the SNI in the client request, or from the CN in the server certificate
B. FortiGate found the requested URL in its local cache.
C. This web request was inspected using the rtgd-allow web filter profile.
D. The requested URL belongs to category ID 255.

Correct Answer: A
Section:
Explanation:
The exhibit displays the output of a real-time debug of the URL filtering process on a FortiGate device. The debug output includes various details about a web request being processed.
SNI (Server Name Indication): This is part of the SSL/TLS handshake where the client specifies the hostname it is trying to connect to. FortiGate can use this information to apply appropriate web filtering rules based on the server name.
CN (Common Name): This is a field in the server's SSL certificate that typically contains the server's hostname. FortiGate can extract this information to verify the identity of the server and apply security policies accordingly.
Given that the debug output includes the hostname 'training.fortinet.com,' it is likely derived from the SNI in the client's request or the CN in the server's certificate, indicating that FortiGate is using this information to process the web request.
Fortinet Community Documentation on Real-time Debugging

QUESTION 14
Refer to the exhibits.

Exhibit 1

```
FGT-A # get router info bgp summary
...
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4      65110    2500    2552        5    0    0 1d11h33m        0
```

Exhibit 2

```
FGT-B # show router bgp
...
    config network
        edit 1
            set prefix 172.16.0.0 255.255.0.0
        next
    end
```

Exhibit 3

```
FGT-B # diagnose ip address  list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.
Which two actions can the administrator take to fix this problem'' (Choose two.)

A. Restart BGP using a soft reset, which forces both peers to exchange their complete BGP routing tables.
B. Manually add the BGP route on FGT-A.
C. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0724.
D. Use the set network-import-check disable command.

Correct Answer: A, D
Section:
Explanation:
Soft Reset of BGP:
Performing a soft reset of BGP is a common method to resolve issues where prefixes are not being received. It forces both BGP peers to resend their complete routing tables to each other.
This can be done using the command: execute router clear bgp soft in and execute router clear bgp soft out.
Network Import Check:
The network-import-check command controls whether the FortiGate should verify that the prefix exists in the routing table before advertising it.
Disabling this check can resolve issues where valid prefixes are not advertised due to stringent verification.
The command to disable this is: config router bgp set network-import-check disable end.
BGP Configuration Verification:
Ensure that the BGP configuration on FGT-B is correctly set to advertise the network 172.16.54.0/24.
Verify that the network statement is correctly configured and matches the intended prefix.
Fortinet Community: Technical Note on Configuring BGP (Welcome to the Fortinet Community!).
Fortinet Documentation: Configuring BGP on FortiGate (Fortinet Document Library).

QUESTION 15
Exhibit.

```
    Chip   XAUI Ports            QSGMII Max   Cross-chip
                                       Speed offloading
    ------ ---- -------          ------ ----- ----------
    np6_0  0    port1            NA     1G    Yes
           0    port5            NA     1G    Yes
           0    port17           NA     1G    Yes
...
```

Refer to the exhibit, which shows the omitted output of diagnose npu np6 port-list on a FortiGate1500D.
An administrator is unable to analyze traffic flowing between port1 and port7 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 0
```

D)

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

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A, C
Section:
Explanation:
Diagnose NPU NP6 Port-list Disable Command:
The diagnose npu np6 port-list disable command disables specific ports on the NP6 processor. This can help in cases where you need to analyze traffic and the hardware offloading is interfering.
Command: diagnose npu np6 port-list disable 5 17 (as shown in Option A).
Diagnose NPU NP6 Fastpath Disable Command:
Disabling the fastpath feature on NP6 can also allow for better visibility into the traffic as it bypasses hardware acceleration, which might obscure traffic details.
Command: diagnose npu np6 fastpath disable 0 (as shown in Option C).
Fortinet Documentation on Troubleshooting BGP and NPU Settings (Fortinet Docs).

Fortinet Community Technical Notes on NPU and Traffic Analysis (Welcome to the Fortinet Community!).

QUESTION 16
Exhibit.

```
# 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
```

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

Correct Answer: D
Section:
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.
Fortinet Documentation: Understanding BGP Route Advertisements (Fortinet Document Library) (Fortinet Docs).

QUESTION 17
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.

Correct Answer: A, B, C
Section:
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.
Fortinet Community: Troubleshooting FSSO Connectivity Issues (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

QUESTION 18
Refer to the exhibit, which shows the output of a diagnose command.
What can you conclude from the RTT value?

A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.
B. Its value is incremented with each packet lost.
C. It determines which FortiGuard server is used for license validation.
D. Its initial value is statically set to 10.

Correct Answer: A
Section:
Explanation:
RTT (Round Trip Time):
RTT in the context of the FortiGuard server list indicates the time it takes for a request to be sent to a FortiGuard server and for a response to be received.
This metric helps determine the latency between the FortiGate device and the FortiGuard servers, which is crucial for ensuring efficient and quick updates and responses for services like web filtering and antivirus updates.
Server Selection:
The FortiGate device uses RTT values to prioritize servers. Servers with lower RTT values are preferred as they respond faster, ensuring minimal delay in processing requests.
This improves the overall performance of FortiGuard services by reducing the time it takes to communicate with the servers.
Fortinet Community: Troubleshooting FortiGuard server connections and RTT values (Welcome to the Fortinet Community!) (Fortinet Docs).
Fortinet Documentation: FortiGuard server settings and RTT explanation (Welcome to the Fortinet Community!) (Fortinet Docs).

QUESTION 19
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0 tun_id=10.200.4.1 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev frag-rfc  accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=2
  src: 0:10.1.2.0/255.255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA:  ref=3 options=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
       ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
  enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
       ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which two statements are correct? (Choose two.)

A. The remote gateway IP is 10.200.5.1.
B. The remote gateway has quick more selectors containing a destination subnet of 10.1.2.0/24.
C. DPD is disabled.
D. Anti-replay is enabled.

Correct Answer: A, D
Section:
Explanation:
Remote Gateway IP:
The output shows 10.200.5.1 as the remote gateway IP, confirming that this is the IP address of the remote gateway involved in the IPsec VPN tunnel.
Quick Mode Selectors:
The quick mode selectors specify the subnets involved in the VPN. The output shows src: 0:10.1.2.0/255.255.255.0:0 and dst: 0:10.1.1.0/255.255.255.0:0, indicating the subnets being tunneled.
DPD (Dead Peer Detection):
DPD is shown as mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0, indicating that DPD is enabled in on-demand mode.
Anti-replay:
The output includes replaywin=2048 and replaywin_lastseq=00000000, which are indicators that anti-replay protection is enabled for the IPsec tunnel.
Fortinet Network Security 7.2 Support Engineer Documentation
VPN Configuration and Diagnostic Guides

QUESTION 20
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.

Correct Answer: B

Section:
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.
Fortinet Documentation on Session Table
Fortinet Community Discussion on Session Table

QUESTION 21
Which statement about IKE and IKE NAT-T is true?

A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.
B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.
C. They each use their own IP protocol number.
D. They both use UDP as their transport protocol and the port number is configurable.

Correct Answer: D
Section:
Explanation:
IKE (Internet Key Exchange): IKE is a protocol used to set up a security association (SA) in the IPsec protocol suite. It is utilized to negotiate, create, and manage SAs.
NAT-T (Network Address Translation-Traversal): NAT-T is used to enable IPsec VPN traffic to pass through NAT devices. It encapsulates IPsec ESP packets into UDP packets.
Transport Protocol: Both IKE and IKE NAT-T use UDP as their transport protocol.
Port Numbers: By default, IKE uses UDP port 500. NAT-T typically uses UDP port 4500. However, these port numbers can be configured as needed.
Fortinet Network Security Support Engineer Study Guide for FortiOS 7.2 (Fortinet Docs) (ebin.pub).
Fortinet Documentation on IPsec VPN Configuration (Fortinet Docs).

QUESTION 22
Refer to the exhibit, which shows the output of a diagnose command

```
# diagnose sys session list expectation
session_info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic (bytes/packets/allow err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426 (10.0.1.10:50365)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos-ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

A. This is an expected session created by the IPS engine.
B. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.
D. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.

Correct Answer: B, D
Section:
Explanation:
Session Creation: The output shows an expected session, likely due to a pinhole, which is a dynamically created rule to allow specific traffic through the firewall.
Routing Decision:
The original direction of traffic comes from the IP address 10.171.121.38.
The next-hop IP address for this traffic is 10.0.1.10 as indicated by the routing decision in the output.
Pinhole Session: Pinhole sessions are typically created for protocols that require additional sessions (e.g., FTP, SIP) to function properly. This ensures the necessary traffic can pass through the firewall.
Debugging Commands: The diagnose sys session list command is used to list session information, which helps in understanding traffic flow and troubleshooting connectivity issues.
Fortinet Network Security Support Engineer Study Guide for FortiOS 7.2 (ebin.pub).
General IPsec VPN configuration from Fortinet documentation (Fortinet Docs).

QUESTION 23
Refer to 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
```

If the default settings are in place, what can you conclude about the conserve mode shown in the exhibit?

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.

Correct Answer: A
Section:
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.

Fortinet Community: Explanation of Conserve Mode and Its Impact (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).
Fortinet Documentation: Conserve Mode Settings and Management (Fortinet Docs).