Free Questions for NSE7_NST-7.2 by certscare

Shared by Trujillo on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Exhibit.

```
FortiGate # get router info routing-table database

Routing table for VRF=0
S           0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S        *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

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
```

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

Why is the port 2 default route not in the second command output?

Options:

A- The port2 interlace is disabled in the FortiGate configuration.

B- The port1 default route has a higher priority value than the default route using port2.

C- The port1 default route has a lower priority value than the default route using port2.

D- The port1 default route has a lower distance than the default route using port2-

Answer:

D

Explanation:

Routing Table Analysis:

The first command output (get router info routing-table database) shows two default routes:

One via port1 with a distance of 10.

One via port2 with a distance of 20.

The second command output (get router info routing-table all) only shows the route via port1.

Administrative Distance:

The administrative distance (AD) is a measure used by routers to select the best path when there are multiple routes to the same destination. The lower the distance, the more preferred the route.

In this scenario, the route via port1 has a lower distance (10) compared to the route via port2 (20), making it the preferred route.

Route Selection:

Since the route via port1 has a lower distance, it is the only one installed in the active routing table, which is why it appears in the second command output, and the port2 route does not.

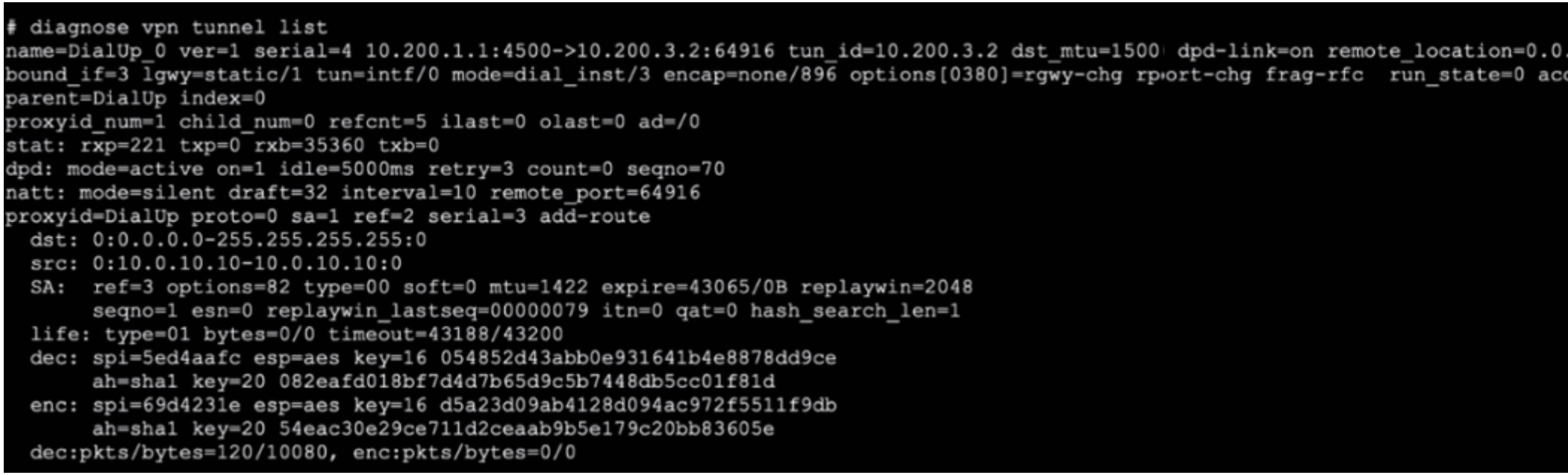
Fortinet Community: Routing behavior depending on distance and priority (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

Fortinet GURU: Route priority and administrative distance explanations (Fortinet GURU).

Question 2

Question Type: **MultipleChoice**

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



```
# diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 acc
parent=DialUp index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=221 txp=0 rxb=35360 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=70
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=3 add-route
  dst: 0:0.0.0.0-255.255.255.255:0
  src: 0:10.0.10.10-10.0.10.10:0
  SA:  ref=3 options=82 type=00 soft=0 mtu=1422 expire=43065/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000079 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=5ed4aafc esp=aes key=16 054852d43abb0e931641b4e8878dd9ce
       ah=sha1 key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01f81d
  enc: spi=69d4231e esp=aes key=16 d5a23d09ab4128d094ac972f5511f9db
       ah=sha1 key=20 54eac30e29ce711d2ceaab9b5e179c20bb83605e
  dec:pkts/bytes=120/10080, enc:pkts/bytes=0/0
```

Which command will capture ESP traffic for the VPN named DialUp_0?

Options:

A- diagnose sniffer packet any 'host 10.0.10.10'

B- diagnose sniffer packet any 'ip proto 50'

C- diagnose sniffer packet any 'esp and host 10*200.3.2'

D- diagnose sniffer packet any 'port 4500'

Answer:

C

Explanation:

Capturing ESP Traffic:

ESP (Encapsulating Security Payload) traffic is associated with IPsec and is identified by the protocol number 50. To capture ESP traffic, you need to filter packets based on this protocol.

In this specific case, you also need to filter for the host associated with the VPN tunnel, which is 10.200.3.2 as indicated in the exhibit.

Sniffer Command:

The correct command to capture ESP traffic for the VPN named DialUp_0 is:

diagnose sniffer packet any 'esp and host 10.200.3.2'

This command ensures that only ESP packets to and from the specified host are captured, providing a focused and relevant data set for troubleshooting.

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

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

Question 3

Question Type: MultipleChoice

Which exchange lakes care of DoS protection in IKEv2?

Options:

A- IKE_Req_INIT

B- IKE_SA_INIT

C- IKE_Auth

D- Create_CHILD_SA

Answer:

B

Explanation:

IKE_SA_INIT Exchange:

The IKE_SA_INIT exchange is the first step in the IKEv2 negotiation process. It is responsible for setting up the initial security association (SA) and performing Diffie-Hellman key exchange.

During this exchange, the responder may employ various measures to protect against Denial of Service (DoS) attacks, such as rate limiting and the use of puzzles to increase the computational cost for an attacker.

DoS Protection Mechanisms:

One key method involves limiting the number of half-open SAs from any single IP address or subnet.

The IKE_SA_INIT exchange can also incorporate the use of stateless cookies, which help to verify the initiator's legitimacy without requiring extensive resource allocation by the responder until the initiator is verified.

RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2) (RFC Editor).

RFC 8019: Protecting Internet Key Exchange Protocol Version 2 (IKEv2) Implementations from Distributed Denial-of-Service Attacks (IETF Datatracker).

Question 4

Question Type: MultipleChoice

Which two statements about application-layer test commands ate true? (Choose two.)

Options:

A- Some of them display statistics and configuration information about a feature or process.

B- Some of them display real-time application debugs.

C- Some of them display only output, after you run the diagnose debug console enable command.

D- Some of them can be used to restart an application.

Answer:

A, B

Explanation:

Statistics and Configuration Information:

Application-layer test commands can display detailed statistics and configuration information about specific features or processes. For example, commands like diagnose vpn ipsec tunnel list provide detailed statistics about VPN tunnels.

Real-time Debugs:

These commands also facilitate real-time debugging of applications and processes. For instance, using diagnose debug application followed by the specific application, such as fssod, provides real-time debug information which is crucial for troubleshooting.

Fortinet Community: Useful FSSO Commands and Troubleshooting (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

Fortinet Documentation: Application-layer Test Commands (Fortinet GURU).

Question 5

Question Type: **MultipleChoice**

Exhibit.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:              type OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:              type-AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id - ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:620000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

Refer to the exhibit, which contains partial output from an IKE real-time debug.

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

Options:

A- In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.

B- In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

C- In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

D- In the phase 1 network configuration, set the IKE version to 2.

Answer:

B

Explanation:

Analyzing Debug Output:

The debug output shows multiple proposals with encryption algorithms like AES CBC and hashing algorithms like SHA256.

The negotiation failure (no SA proposal chosen) suggests that there is a mismatch in the encryption or hashing algorithms between the local and remote gateways.

Configuration Change:

To resolve the phase 1 negotiation error, the local gateway needs to include a compatible proposal.

Adding AES256-SHA256 to the phase 1 proposal configuration ensures that both gateways have a matching set of encryption and hashing algorithms.

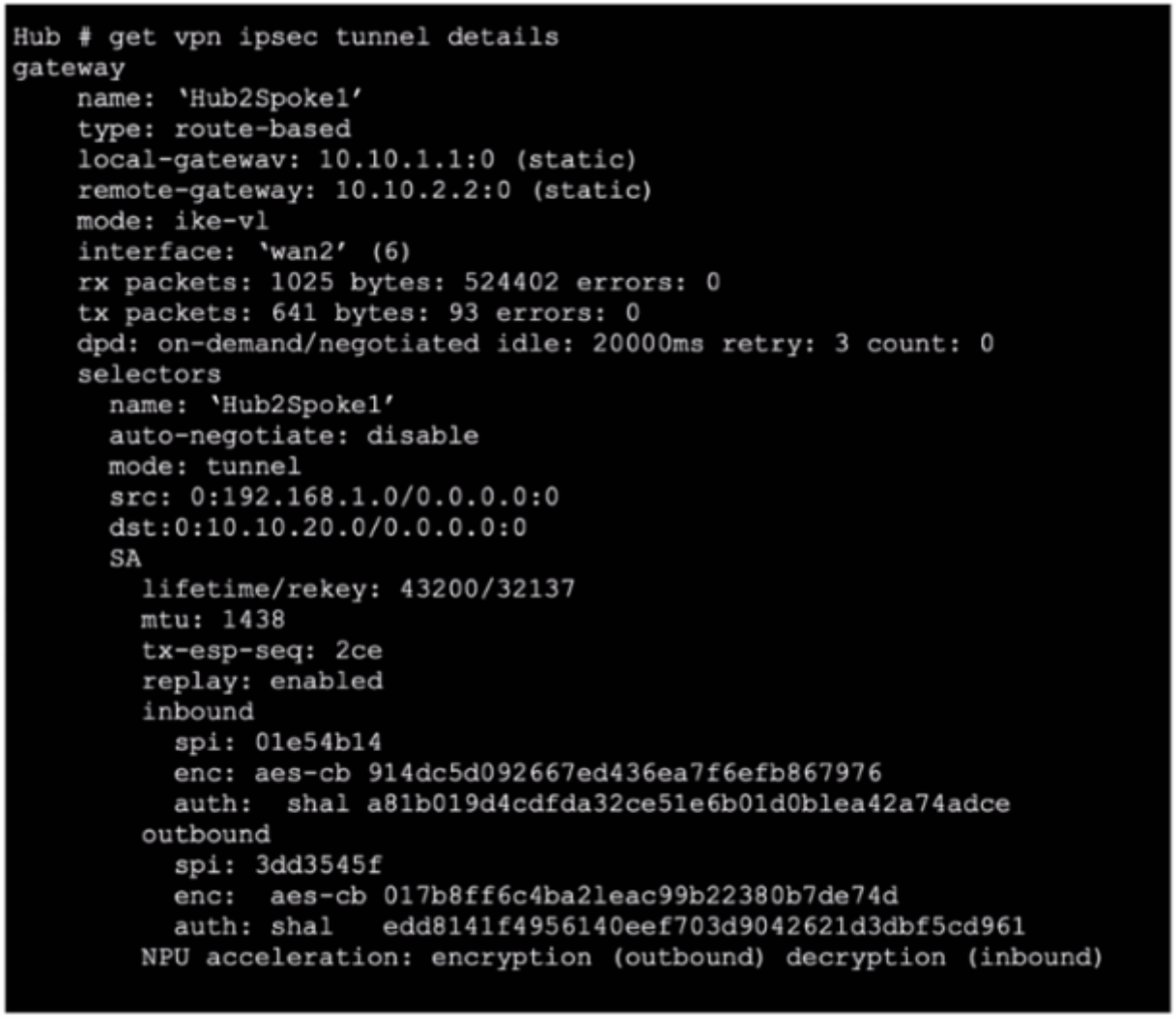
Fortinet Documentation: Configuring IPsec Tunnels (Fortinet Docs) (Welcome to the Fortinet Community!).

Fortinet Community: Troubleshooting IKE Negotiation Failures (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

Question 6

Question Type: **MultipleChoice**

Exhibit.



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.)

Options:

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.

Answer:

A, C

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 7

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 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.

Answer:

A

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 8

Question Type: MultipleChoice

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.)

Options:

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:

C, D

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 9

Question Type: MultipleChoice

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

Options:

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:

A, B, C

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 10

Question Type: MultipleChoice

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?

Options:

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.

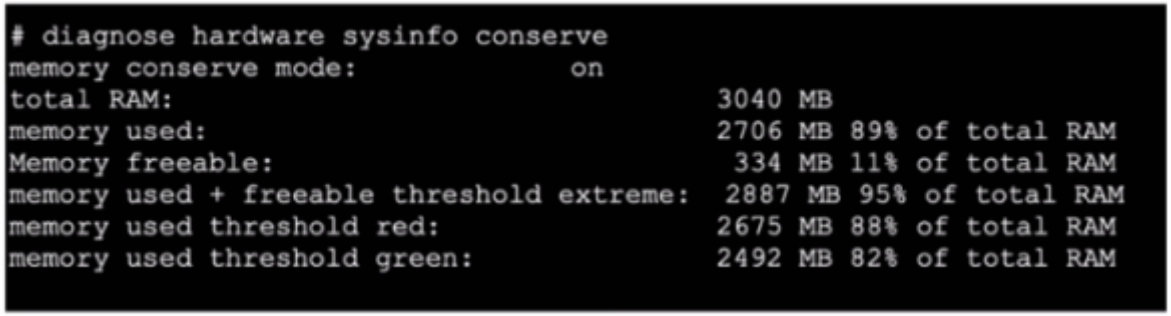
This confirms that the local router is indeed advertising the specified network to its BGP neighbor.

Fortinet Documentation: Understanding BGP Route Advertisements (Fortinet Document Library) (Fortinet Docs).

Question 11

Question Type: MultipleChoice

Refer to the exhibit.



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

Options:

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.

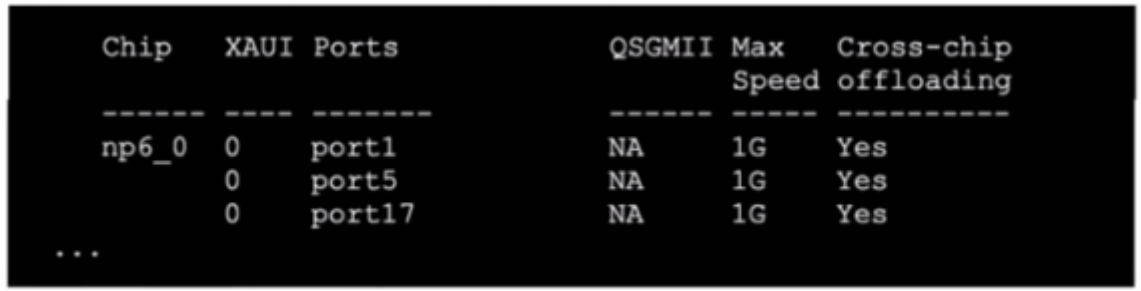
Fortinet Community: Explanation of Conserve Mode and Its Impact (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

Fortinet Documentation: Conserve Mode Settings and Management (Fortinet Docs).

Question 12

Question Type: **MultipleChoice**

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
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

A, C

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!).