

Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer



NEW QUESTION 1

Refer to the exhibits.

```
FGT-B # get router info routing-table all
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 192.168.1.1, port1, [1/0]
C     10.23.23.0/24 is directly connected, port4
```

```
FGT-B # get router info ospf database brief
...
AS External Link States

Link ID      ADV Router   Age  Seq#       CkSum  Flag Route      Tag
8.8.8.8      0.0.0.112   1464 80000002  3106   0002 E2 8.8.8.8/32    0
```

An administrator is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT-B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

- A. A better route to the 8.8.8.8/32 network exists in the routing table.
- B. FGT-B is configured with a prefix list denying the 8.8.8.8/32 network to be injected into the routing table.
- C. The administrator has misconfigured redistribution of routes on FGT-A.
- D. FGT-B is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

NEW QUESTION 2

Exhibit.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-id6 ::
    set proxv-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dns-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator do to fix the issue?

- A. Disable webfilter-force-off.
- B. Increase webfilter-timeout.
- C. Enable fortiguard-anycast.
- D. Change protocol to TCP.

Answer: A

NEW QUESTION 3

Refer to the exhibit, which shows the output of diagnose sys session list.

Diagnose output

```
# 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/ff ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

- A. 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.
- B. 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.
- C. 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.
- D. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

Answer: B

NEW QUESTION 4

Exhibit 1.

```
config system global
    set snat-route-change disable
end

config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= 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=log may_dirty npu f00
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=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
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
no_ofld_reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network. An administrator would like to test session failover between the two service provider connections.

Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

- A. Change the priority of the port1 static route to 11.
- B. Change the priority of the port2 static route to 5.
- C. Configure unset snat-route-change to return it to the default setting.
- D. Configure set snat-route-change enable.

Answer: AD

NEW QUESTION 5

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

Answer: D

Explanation:

When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, FortiGate does not block the connection; instead, it uses the CN value from the certificate's subject field to continue web filtering and categorization.

This behavior is described in the official Fortinet 7.6.4 Administration Guide:

"Check the SNI in the hello message with the CN or SAN field in the returned server certificate: Enable: If it is mismatched, use the CN in the server certificate."

This is the default (Enable) mode, which differs from the Strict mode that would block the mismatched connection.

By default, this policy ensures service continuity and prevents disruptions due to certificate mismatches, allowing FortiGate to log and inspect based on the CN even when the requested SNI does not match. It provides a balance between connection reliability and the accuracy of filtering by certificate identity, allowing security policies to remain functional without unnecessary blocks. This approach is recommended by Fortinet to maintain usability for end-users while still supporting granular inspection.

[References: FortiGate 7.6.4 Administration Guide: Certificate Inspection?, SSL/SSH Inspection Profile Configuration,]

NEW QUESTION 6

Refer to the exhibits, which contain the partial configurations of two VPNs on FortiGate.

Exhibit 1

```
config vpn ipsec phase1-interface
edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

Exhibit 2

```
config vpn ipsec phase1-interface
edit "user-2"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-2"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovers that FortiGate is not matching the user-2 VPN for members of the Users-2 group. Which two changes must the administrator make to fix the issue? (Choose two.)

- A. Change to aggressive mode on both VPNs.
- B. Enable XAuth on both VPNs.
- C. Use different pre-shared keys on both VPNs.
- D. Set up specific peer IDs on both VPNs.

Answer: AD

NEW QUESTION 7

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

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

Answer: BCD

NEW QUESTION 8

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=0.0.0.0 weight=1
bound if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encaps=none/896 options[0380]=rgwy-chg rport-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0
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?

- A. diagnose sniffer packet any 'ip proto 50'
- B. diagnose sniffer packet any 'host 10.0.10.10'
- C. diagnose sniffer packet any 'esp and host 10.200.3.2'
- D. diagnose sniffer packet any 'port 4500'

Answer: D

NEW QUESTION 9

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. diagnose sniffer packet any 'udp port 500'
- B. diagnose sniffer packet any 'ip proto 50'
- C. diagnose sniffer packet any 'udp port 4500'
- D. diagnose sniffer packet any 'ah'

Answer: B

NEW QUESTION 10

Which statement about protocol options is true?

- A. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
- B. Protocol options give administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
- C. Protocol options allow administrators to configure the Any setting for all enabled protocols, which provides the most efficient use of system resources.
- D. Protocol options allow administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

Answer: D

NEW QUESTION 10

Exhibit.

```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 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
user=User1 state=log may_dirty authenticated f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason: npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Two.)

- A. The TCP session has been successfully established.
- B. The session was initiated from an authenticated user.
- C. The session is being inspected using flow inspection.
- D. The session is being offloaded.

Answer: AB

NEW QUESTION 14

Which statement about parallel path processing is correct (PPP)?

- A. PPP chooses from a group of parallel options to identify the optimal path for processing a packet.
- B. Only FortiGate hardware configurations affect the path that a packet takes.
- C. PPP does not apply to packets that are part of an already established session.

D. Software configuration has no impact on PPP.

Answer: A

Explanation:

Parallel Path Processing (PPP) in FortiOS refers to the system's ability to evaluate and select among multiple processing paths—often involving dedicated network processors, content processors, or CPU-based workflows—to optimally process packets. The official documentation highlights that the PPP engine dynamically selects which hardware or software path to use for each session based on session characteristics, policy configuration, and traffic type. This dynamic selection results in optimal throughput and resource utilization.

The document specifies that PPP assesses several processing paths in parallel, using decision logic to determine whether a session should be offloaded to specialist hardware (like NP6, CP9, etc.) or stay in the CPU path, ensuring that each packet is handled by the most efficient available method under current load and policy. Hardware and software configurations both influence this outcome, but it is the PPP engine's decision-making that defines the optimal path per session. [References:, Fortinet FortiGate Handbook: Parallel Path Processing, Fortinet FortiOS Technical Documentation: Packet Flow and Path Selection,]

NEW QUESTION 19

Exhibit.

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

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

What three conclusions can you draw from these log entries? {Choose three.}

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

Answer: ABE

NEW QUESTION 22

Refer to the exhibit, which shows the output of the command `get router info bgp neighbors 100.64.2.254 advertised-routes`.

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

Answer: D

NEW QUESTION 24

Which two statements about Security Fabric communications are true? (Choose two.)

- A. FortiTelemetry and Neighbor Discovery both operate using TCP.
- B. The default port for Neighbor Discovery can be modified.
- C. FortiTelemetry must be manually enabled on the FortiGate interface.
- D. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.

A.

Answer: CD

Explanation:

FortiTelemetry is a critical part of Security Fabric communications and requires explicit configuration for each participating FortiGate interface. The administrative access setting 'fabric' (corresponding to FortiTelemetry) must be manually enabled per interface on both upstream and downstream devices. This is performed in the GUI under Administrative Access or via the CLI using the commandset `allowaccess fabric` for the relevant network interface. Without this step, FortiTelemetry communications will not occur on that interface.

Additionally, the default communication between downstream and upstream FortiGate units in the Security Fabric is over TCP port 8013. This port is well-documented as the standard for Security Fabric and FortiTelemetry connections, and must be open and permitted across the network path for connectivity and status enforcement between units. The downstream FortiGate initiates the connection to the upstream via this port unless otherwise configured. This has also been documented as a PCI-relevant port, showing its default usage.

Other options:

Neighbor Discovery in FortiOS uses IPv6 ND protocol, not TCP.

FortiTelemetry port (8013) can be modified, but the interface Administrative Access for the Security Fabric must be manually enabled; Neighbor Discovery port modification is not documented as a supported change for FortiGate.

FortiGate/FortiOS Administration Guide: Enabling FortiTelemetry (fabric) on interfaces

Fortinet Technical Tip: FortiTelemetry uses TCP port 8013 by default

PCI compliance documentation on port 8013 usage for Security Fabric

Fortinet Security Fabric setup procedures and interface options

NEW QUESTION 28

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

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60    4      65060   1698   1756     103    0    0 03:02:49      1
10.127.0.75    4      65075   2206   2250     102    0    0 02:45:55      1
100.64.3.1     4      65501    101    115      0      0    0 never      Active

Total number of neighbors 3
```

What can you conclude about the router in this scenario?

- A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the BGP session with the local router.
- B. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1.
- C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
- D. The BGP session with peer 10.127.0.75 is up.

A.

Answer: D

Explanation:

The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show 'Idle,' 'Active,' or 'Connect,' but instead shows 'Established,' 'Up,' or related counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.

The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.

FortiOS BGP Debugging Guide: Session State Interpretation

BGP CLI Reference: Neighbor Status Fields

NEW QUESTION 33

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

Routing information

```
# 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, [1/0]
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 egress interface associated with static route 8.8.8.8/32 is administratively up.
- B. The default static route through 10.200.1.254 is not in the forwarding information base.
- C. The default static route through port2 is in the forwarding information base.
- D. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

A.

Answer: D

NEW QUESTION 36

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. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.
- B. Manually add the BGP route on FGT-A.
- C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
- D. Use the set network-import-check disable command.

Answer: AD

NEW QUESTION 40

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

```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
100.64.1.254   4      100    18     20      3    0    0 00:02:55      1
100.64.2.254   4      100     0      0      0    0    0 never      Active

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

- A. The local FortiGate has received one prefix from BGP neighbor 100.64.1.254.
- B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
- C. The local FortiGate has received 18 packets from a BGP neighbor.
- D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: AC

Explanation:

The get router info bgp summary output lists BGP neighbor status:

Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.

Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.

The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B. There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect. [References:, , FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters]

NEW QUESTION 42

In IKEv2, which exchange establishes the first CHILD_SA?

- A. IKE_SA_INIT
- B. INFORMATIONAL
- C. CREATE_CHILD_SA
- D. IKE_Auth

Answer: A

Explanation:

According to RFC 7296 (IKEv2) and Fortinet's official documentation, theIKE_SA_INIT exchangeis responsible for negotiating cryptographic parameters, performing the initial Diffie-Hellman exchange, and implementing the cookie challenge mechanism for DoS protection. When the responder suspects a DoS attack (such as mass requests by the same source), it includes a cookie in the IKE_SA_INIT response. The initiator must return the cookie in its next request to prove that it truly exists at the IP address it claims, thereby mitigating resource exhaustion attacks. This two-step exchange ensures the responder only allocates resources after successful proof of address, aligning with best security practices. Fortinet documentation confirms that this process occurs strictly in the IKE_SA_INIT phase, not in subsequent IKE_Auth or CHILD_SA exchanges. [References:, RFC 7296: IKEv2, Section 2.6, ??Denial of Service Protection?, Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism, , ,]

NEW QUESTION 47

Exhibit.

FGT # diagnose debug rating													
Locale : english													
Service : Web-filter													
Status : Enable													
License : Contract													
Service : Antispam													
Status : Disable													
Service : Virus Outbreak Prevention													
Status : Disable													
Num. of servers : 1													
Protocol : https													
Port : 443													
Anycast : Enable													
Default servers : Included													
--- Server List (Mon May 1 03:47:52 2023) ---													
IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr	Lost	Total	Lost	Updated Time			
64.26.151.37	10	45		-5	262432		0		846	Mon May	1	03:47:43	2023
64.26.151.35	10	46		-5	329072		0		6806	Mon May	1	03:47:43	2023
66.117.56.37	10	75		-5	71638		0		275	Mon May	1	03:47:43	2023
65.210.95.240	20	71		-8	36875		0		92	Mon May	1	03:47:43	2023
209.22.147.36	20	103	DI	-8	34784		0		1070	Mon May	1	03:47:43	2023
208.91.112.194	20	107	D	-8	35170		0		1533	Mon May	1	03:47:43	2023
				0	33728		0		120	Mon May	1	03:47:43	2023
				1	33797		0		192	Mon May	1	03:47:43	2023
				9	33754		0		145	Mon May	1	03:47:43	2023
				-5	26410			26226	26227	Mon May	1	03:47:43	2023

Refer to the exhibit, which shows the output of a diagnose command. What can you conclude about the debug output in this scenario?

- A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.
- B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.
- C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
- D. Servers with a negative TZ value are less preferred for rating requests.

Answer: C

Explanation:

The exhibit displays the output from the diagnose debug rating command on a FortiGate device. This command is used to display information about FortiGuard Web Filtering or other security-related queries performed by FortiGate to FortiGuard servers. Official Fortinet documentation outlines the meaning of each field in the server list. The FortiGate maintains a list of available FortiGuard servers, selecting the optimal server based on factors such as weight, round-trip time (RTT), and regional settings. The very first entry in the server list after "Server List" is the server FortiGate initially uses, prioritized by factors such as proximity and RTT. Here, 64.26.151.37 is listed first, and the FortiGuard-requests value confirms that this server handled the highest number of requests. The IPs, weights, and lost/failed counters are monitored for server performance and selection over time. FortiGate's default operational logic is to try the first entry for contract validation and use the next in the list if the first is unavailable or has high latency or packet loss. There is no direct correlation between the Weight and the number of FortiGuard-requests. The servers with higher or lower weights may still handle different request volumes based on availability and performance. The TZ (time zone) value's sign (positive or negative) does not affect server preference; it is informational, showing the server's location relative to UTC, not a rating metric. DNS query results for FortiGuard servers are not shown here, and the provided servers are not returned in DNS query order. This command and interpretation are detailed in the FortiOS Administration Guide's section describing FortiGuard server selection and contract validation processes. [References:, , FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging, , Official Technical Notes on diagnose debug rating output structure]

NEW QUESTION 50

Which two statements are true regarding heartbeat messages sent from an FSSO collector agent to FortiGate? (Choose two.)

- A. The heartbeat messages can be seen using the command diagnose debug authd fsso list.
- B. The heartbeat messages can be seen in the collector agent logs.
- C. The heartbeat messages can be seen on FortiGate using the real-time FSSO debug.
- D. The heartbeat messages must be manually enabled on FortiGate.

Answer: BC

Explanation:

According to the official Fortinet documentation (Technical Tip: Useful FSSO Commands), heartbeat messages play a crucial role in communication between the FSSO Collector Agent and FortiGate. These messages are regularly sent from the Collector Agent to verify its status, maintain session awareness, and confirm connectivity between the authentication infrastructure and FortiGate appliances.

Option B is confirmed by Fortinet, as the collector agent logs on Windows or its management console will specifically note heartbeat events, connection status, and any issues maintaining contact with FortiGate units.

Option C is validated by both official CLI documentation and the technical tip linked. On FortiGate, heartbeat messages from the collector agent are visible using real-time debug tools such asdiagnose debug application authdor FSSO-specific commands. These enable administrators to monitor live logon states, session status, and connection health directly from the FortiGate CLI. The debug stream shows heartbeats received and their effect on active logons, associating health monitoring with active sessions.

Heartbeat operation is fully automated once FSSO is set up—there is no requirement for manual enablement or configuration, aligning with Fortinet’s philosophy of seamless integration and centralized management across the Security Fabric. This ensures that both FortiGate and the collector agent can quickly and reliably detect any miscommunication or outage, addressing authentication issues proactively.

[References:, Technical Tip: Useful FSSO Commands (Fortinet Community)?, FortiOS Administration Guide: FSSO, Collector Agent, Heartbeat, CLI Debug,]

NEW QUESTION 55

Refer to the exhibit, which shows the partial output of command diagnose debug rating.

-- Server List (Mon May 6 03:47:52 2024) --										
IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr	Lost	Total	Lost	Updated Time
64.26.151.37	10	45		-5	262432		0	846	Mon May 6 03:47:43 2024	
64.26.151.35	10	46		-5	329072		0	6806	Mon May 6 03:47:43 2024	
66.117.56.37	10	75		-5	71638		0	275	Mon May 6 03:47:43 2024	
65.210.95.240	20	71		-8	36875		0	92	Mon May 6 03:47:43 2024	
209.22.147.36	20	103	DI	-8	34784		0	1070	Mon May 6 03:47:43 2024	
208.91.112.194	20	107	D	-8	35170		0	1533	Mon May 6 03:47:43 2024	
96.45.33.65	60	144		0	33728		0	120	Mon May 6 03:47:43 2024	
80.85.69.41	71	226		1	33797		0	192	Mon May 6 03:47:43 2024	
62.209.40.74	150	97		9	33754		0	145	Mon May 6 03:47:43 2024	
121.111.236.179	45	44	F	-5	26410		26226	26227	Mon May 6 03:47:43 2024	

- A. 66.117.56.37
- B. 208.91.112.194
- C. 209.22.147.36
- D. 64.26.151.37

Answer: D

NEW QUESTION 59

Which two statements about an auxiliary session ate true? (Choose two.)

- A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.
- B. With the auxiliary session setting enable
- C. ECMP traffic is accelerated to the NP6 processor.
- D. With the auxiliary session setting enable
- E. Iwo sessions are created in case of routing change.
- F. With the auxiliary session setting disabled, for each traffic pat
- G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 61

During which phase of IKEv2 does the Diffie-Helman key exchange take place?

- A. IKE_Req_INIT
- B. Create_CHILD_SA
- C. IKE_Auth
- D. IKE_SA_INIT

Answer: D

NEW QUESTION 65

Exhibit.


```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
<2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
FGVM010000077649(updated 4 seconds ago): in-sync
FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
FGVM010000077649(updated 4 seconds ago):
sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
FGVM010000077650(updated 1 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
FGVM010000077649(updated 4 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
FGVM010000077650(updated 1 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary : NGFW-1 , FGVM010000077649, HA cluster index = 1
Secondary : NGFW-2 , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

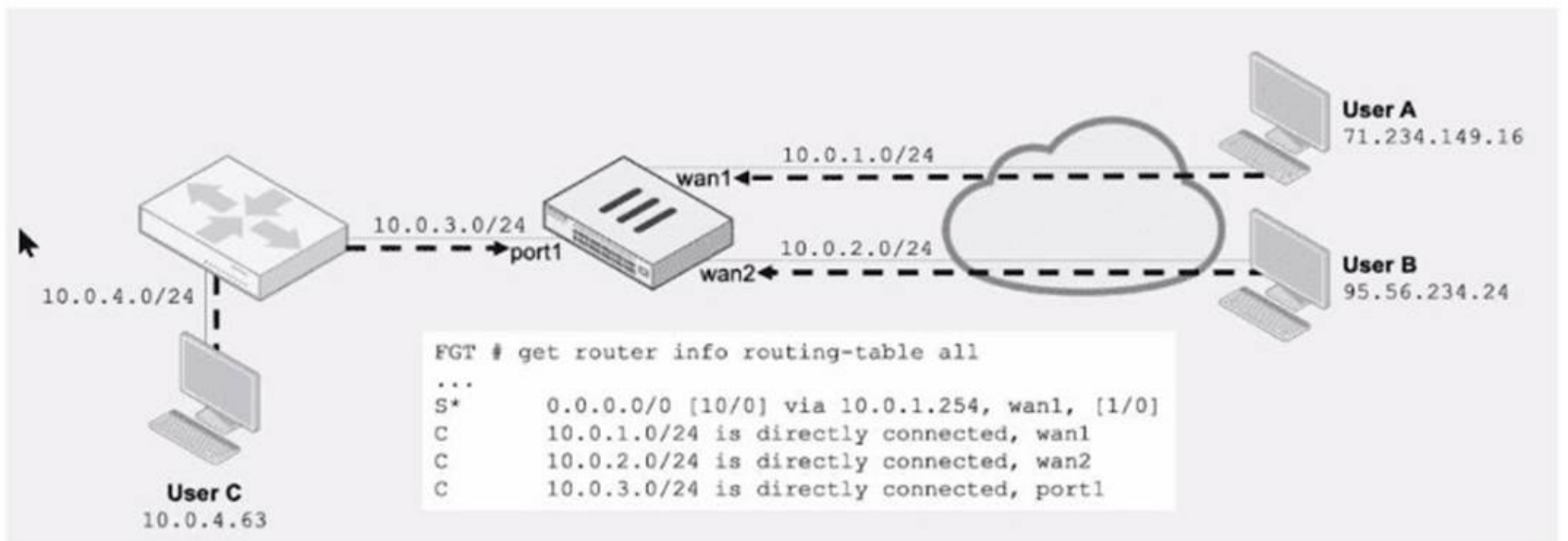
Refer to the exhibit, which shows the output of get system ha status. NGFW-1 and NGFW-2 have been up for a week. Which two statements about the output are true? (Choose two.)

- A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.
- B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.
- C. If FGVM...649 is rebooted
- D. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
- E. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Answer: BC

NEW QUESTION 69

Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three.)

- A. Strict RPF is enabled by default.
- B. User B: Fai
- C. There is no route to 95.56.234.24 using wan2 in the routing table.
- D. User A: Pas
- E. The default static route through wan1 passes the RPF check regardless of the source IP address.
- F. User B: Pas
- G. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
- H. User C: Fai
- I. There is no route to 10.0.4.63 using port1 in the routing table.

Answer: BDE

NEW QUESTION 70

In the SAML negotiation process, which section does the Identity Provider (IdP) provide the SAML attributes utilized in the authentication process to the Service Provider (SP)?

- A. SP Login dump
- B. Authentication Response
- C. Authentication Request
- D. Assertion dump

Answer: D

NEW QUESTION 74

Refer to the exhibit, which shows the output of get router info ospf neighbor.

```
Spokel # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID    Pri   State           Dead Time   Address      Interface
0.0.0.1        1     Full/DR         00:00:39    10.10.2.1    wan1
0.0.0.3        1     Full/DROther    00:00:37    10.10.3.2    wan2
0.0.0.10       c1    Full/-          00:00:36    172.16.1.2   ToHub
```

What can you conclude from the command output?

- A. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to- point.
- B. All neighbors are in area 0.0.0.0.
- C. The local FortiGate is the BDR.
- D. The local FortiGate is not a DROther.

Answer: A

NEW QUESTION 75

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

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

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
          [10/0] via 100.64.2.254, port2, [10/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.10.0/24 [10/0] via 10.1.0.1, port3
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- A. Set snat-route-change to enable.
- B. Set the priority of the static default route using port2 to 1.
- C. Set preserve-session-route to enable.
- D. Set the priority of the static default route using port1 to 10.

Answer: D

NEW QUESTION 78

What are two functions of automation stitches? (Choose two.)

- A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
- B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
- C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
- D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Answer: BD

NEW QUESTION 83

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCSS_NST_SE-7.6 Practice Exam Features:

- * FCSS_NST_SE-7.6 Questions and Answers Updated Frequently
- * FCSS_NST_SE-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_NST_SE-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_NST_SE-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_NST_SE-7.6 Practice Test Here](#)