

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

https://www.2passeasy.com/dumps/FCSS_NST_SE-7.6/



NEW QUESTION 1

What are two reasons you might see iprope_in_check() check failed, drop when using the debug flow? (Choose two.)

- A. Packet was dropped because of policy route misconfiguration.
- B. Packet was dropped because of traffic shaping.
- C. Trusted host list misconfiguration.
- D. VIP or IP pool misconfiguration.

Answer: CD

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
origin->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
rpdb_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
vlid=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 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 encap=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 7

The local OSPF router is unable to establish adjacency with a peer.

Which two things should the administrator do to troubleshoot the issue? (Choose two.)

- A. Check whether TCP port 179 is blocked.
- B. Check if there is an active static route to the peer.
- C. Check whether both peers have an IP address within the same subnet.
- D. Check if IP protocol 89 is blocked.

Answer: CD

NEW QUESTION 8

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 9

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

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
Process ID 0, VRF 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROther, Priority 1

Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2

Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:05
Neighbor Count is 4, Adjacent neighbor count is 2
Crypt Sequence Number is 411
Hello received 106 sent 27, DD received 6 sent 3
LS-Req received 2 sent 2, LS-Upd received 7 sent 17
LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

- A. The interlace is part of the OSPF backbone area.
- B. There are a total of five OSPF routers attached to the vorz4 network segment
- C. One of the neighbors has a router ID of 0.0.0.4.
- D. In the network connected to port4, two OSPF routers are down.

Answer: AB

Explanation:

FortiOS Admin Guide: OSPF, Debug Outputs

NEW QUESTION 10

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 10

Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

```

config system interface
  edit "port1"
    set preserve-session-route enable
  next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state-log may_dirty npu f00 route_preserve
origin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0

```

What happens to the session information if a routing change occurs that affects this session?

- A. Only the interface and gateway information for dev=7 will be removed.
- B. The session information will not change unless the current route has been removed from the routing table.
- C. The session will be flagged as dirty but no route lookups will be performed.
- D. Sessions involving port7 or port19 will not have their routing information flushed.

A.

Answer: B

NEW QUESTION 11

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

```

Which statement is true?

- A. The 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 14

Refer to the exhibit.

```

**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC719A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><saml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL30W5sAZtBwhhEEtQF0AdfTN0u0GRr22%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC719A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>

```

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.

Based on this output, what can you conclude?

- A. Active Directory is used for authentication.
- B. The authentication request is for an SSL VPN connection.
- C. The IdP IP address is 10.1.10.254.
- D. The IdP IP address is 10.1.10.2.

A.

Answer: D

NEW QUESTION 15

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     -5  262432                0         0      846  Mon May 1 03:47:43 2023
64.26.151.35 10      46   -5     -5  329072                0         0      6806 Mon May 1 03:47:43 2023
66.117.56.37 10      75   -5     -5  71638                 0         0      275  Mon May 1 03:47:43 2023
65.210.95.240 20     71   -8     -8  36875                 0         0      92   Mon May 1 03:47:43 2023
209.22.147.36 20    103  DI    -8  34784                 0         0     1070 Mon May 1 03:47:43 2023
208.91.112.194 20    107  D     -8  35170                 0         0     1533 Mon May 1 03:47:43 2023
              0      0     0     0  33728                 0         0      120  Mon May 1 03:47:43 2023
              1      0     0     0  33797                 0         0      192  Mon May 1 03:47:43 2023
              9      0     0     0  33754                 0         0      145  Mon May 1 03:47:43 2023
              -5     0     0     0  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 16

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 as diagnose debug application authd or 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 20

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 22

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
```

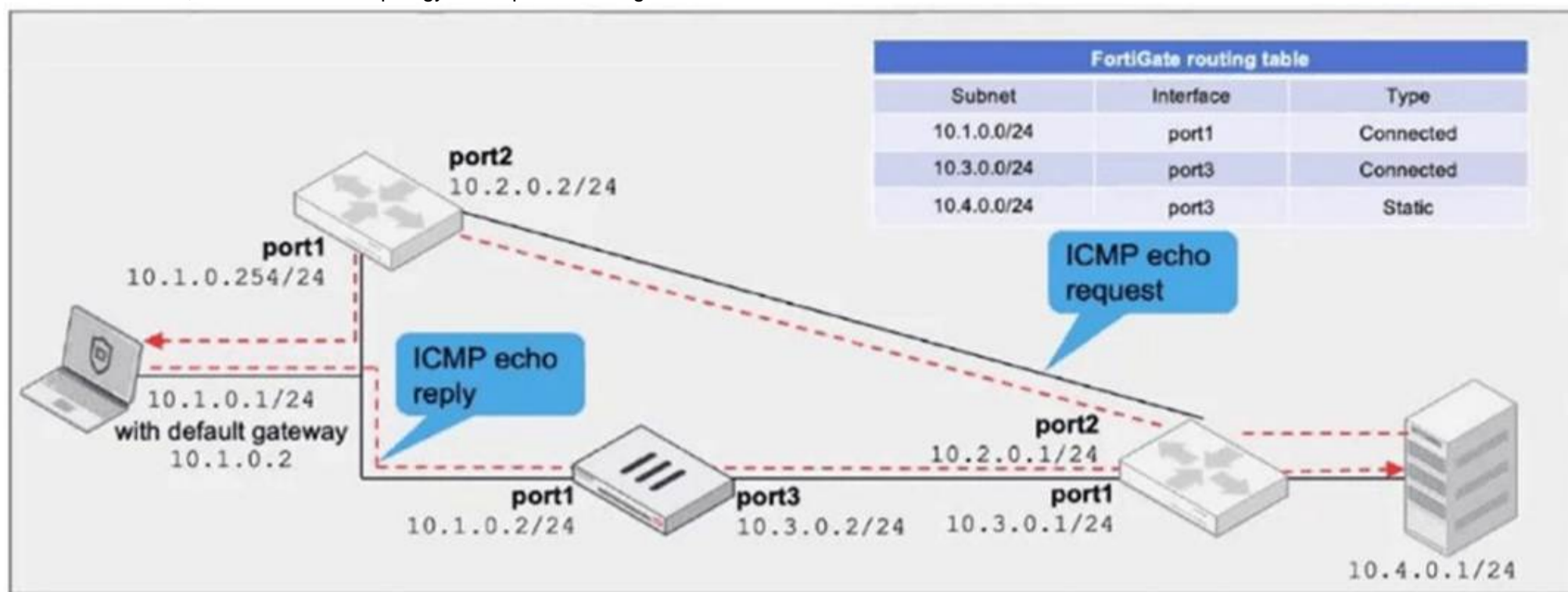
Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- 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 25

Refer to the exhibit, which a network topology and a partial routing table.



FortiGate has already been configured with a firewall policy that allows all ICMP traffic to flow from port1 to port3. Which changes must the administrator perform to ensure the server at 10.4.0.1/24 receives the echo reply from the laptop at 10.1.0.1/24?

- A. Enable asymmetric routing under config system settings.
- B. Change the configuration from strict RPF check mode to feasible RPF check mode.
- C. A firewall policy that allows all ICMP traffic from port3 to port1.
- D. Modify the default gateway on the laptop from 10.1.0.2 to 10.2.0.2.

Answer: A

NEW QUESTION 28

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_NST_SE-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_NST_SE-7.6 Product From:

https://www.2passeasy.com/dumps/FCSS_NST_SE-7.6/

Money Back Guarantee

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