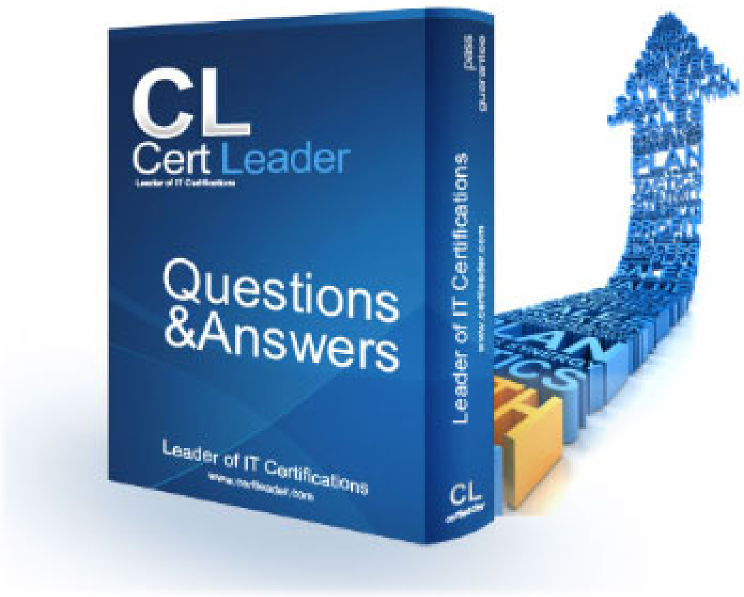
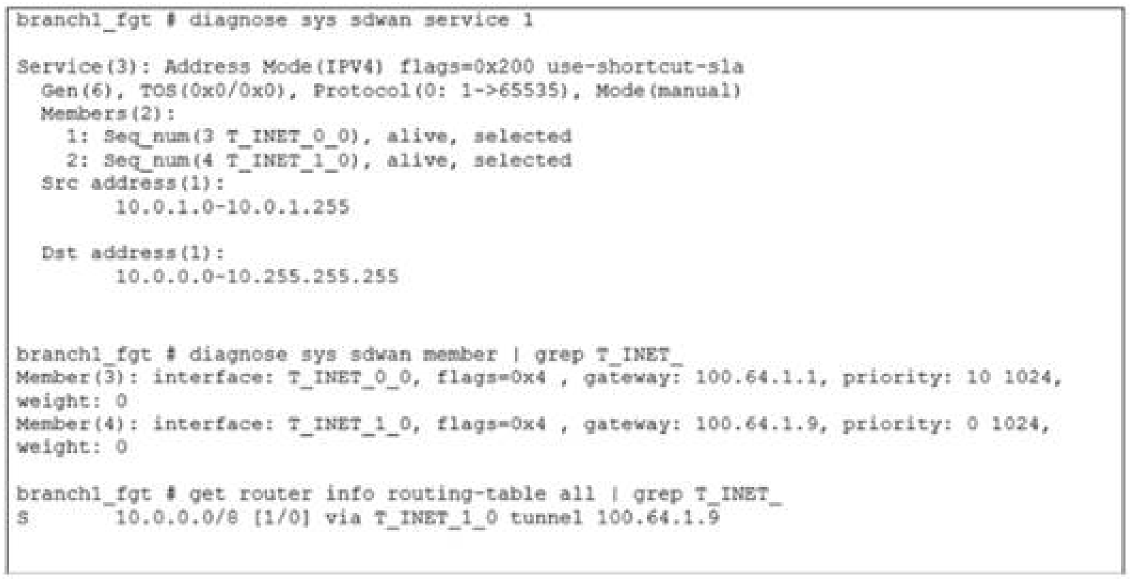
NSE7_SDW-7.2 Dumps

Fortinet NSE 7 - SD-WAN 7.2

https://www.certleader.com/NSE7_SDW-7.2-dumps.html



NEW QUESTION 1
Refer to the exhibit.



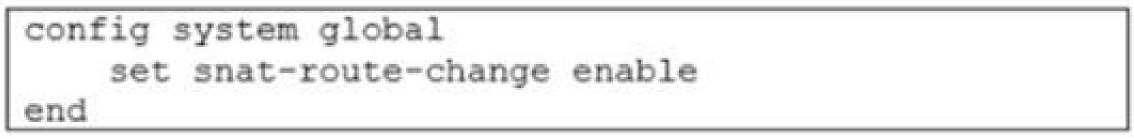
```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(3 T_INET_0_0), alive, selected
    2: Seq_num(4 T_INET_1_0), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S       10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T_INET_0_0. However, the traffic is routed over T_INET_1_0.
Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. The traffic matches a regular policy route configured with T_INET_1_0 as the outgoing device.
B. T_INET_1_0 has a lower route priority value (higher priority) than T_INET_0_0.
C. T_INET_0_0 does not have a valid route to the destination.
D. T_INET_1_0 has a higher member configuration priority than T_INET_0_0.

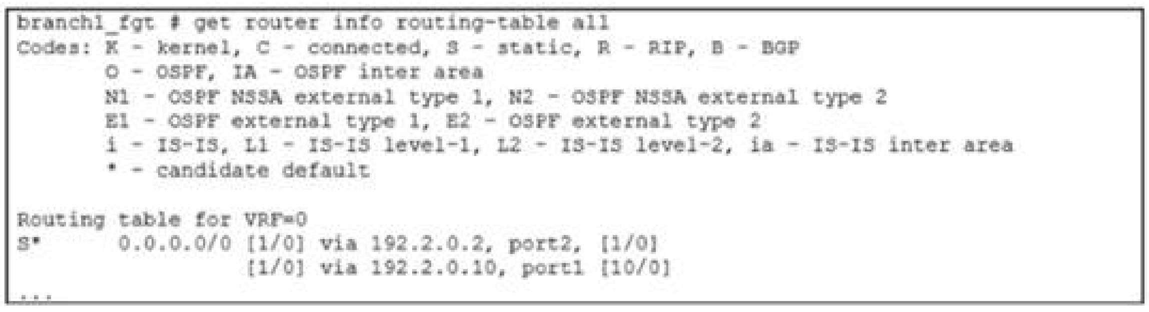
Answer: AC

NEW QUESTION 2
Refer to the exhibits.
Exhibit A



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

Exhibit B



```
branch1_fgt # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
                  [1/0] via 192.2.0.10, port1 [10/0]
...
```

Exhibit A shows the source NAT (SNAT) global setting and exhibit B shows the routing table on FortiGate.
Based on the exhibits, which two actions does FortiGate perform on existing sessions established over port2, if the administrator increases the static route priority on port2 to 20? (Choose two.)

A. FortiGate flags the sessions as dirty.
B. FortiGate continues routing the sessions with no SNAT, over port2.
C. FortiGate performs a route lookup for the original traffic only.
D. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: BD

NEW QUESTION 3
Which action fortigate performs on the traffic that is subject to a per-IP traffic shaper of 10 Mbps?

A. FortiGate applies traffic shaping to the original traffic direction only.
B. FortiGate shares 10 Mbps of bandwidth equally among all source IP addresse
C. RIAS
D. Fortigate limits each source ip address to a maximum bandwidth of 10 Mbps.
E. FortiGate guarantees a minimum of 10 Mbps of bandwidth to each source IP address.

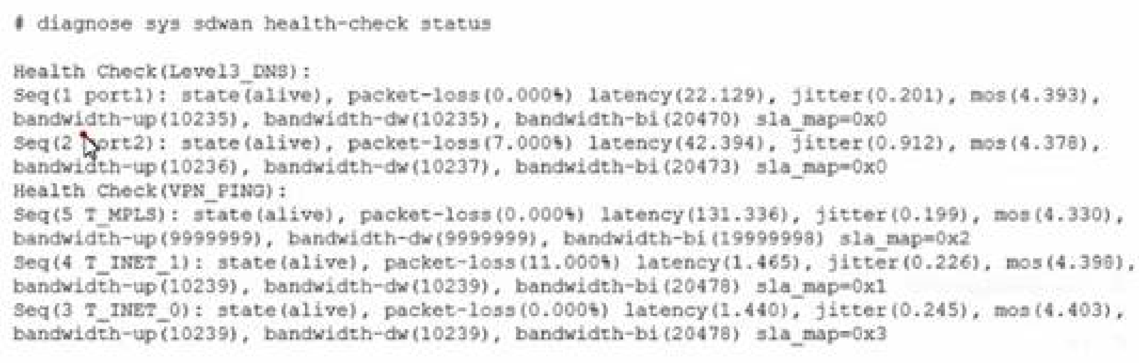
Answer: C

NEW QUESTION 4
Which are two benefits of using CLI templates in FortiManager? (Choose two.)

A. You can reference meta fields.
B. You can configure interfaces as SD-WAN members without having to remove references first.
C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
D. You can configure advanced CLI settings.

Answer: AD

NEW QUESTION 5
Exhibit.



```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The exhibit shows the output of the command diagnose sys sdwan health-check status
collected on a FortiGate device. Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

A. The health-check VPN_PING orders the members according to the lowest jitter.
B. The interface T_INET_1 missed one SLA target.
C. There is no SLA criteria configured for the health-check Level3_DNS.
D. The interface T_INET_0 missed three SLA targets.

Answer: AC

Explanation:
According to the FortiGate / FortiOS 6.4.2 Administration Guide, the health check status command displays the status of the health check probes for each SD-WAN member interface. The output includes the following information:
? state: the current state of the interface, either alive or dead
? packet-loss: the percentage of packets lost during the health check
? latency: the average round-trip time in milliseconds
? jitter: the variation in latency
? mos: the mean opinion score, a measure of voice quality
? bandwidth: the available bandwidth in kilobits per second for each direction (up, down, bi)
? sla map: a bitmap that indicates which SLA criteria are met or failed Based on the exhibit, the following statements are correct:
? The health-check VPN_PING orders the members according to the lowest jitter. This means that the interface with the lowest jitter value is listed first, followed by the next lowest, and so on1. In the exhibit, the order is T_MPLS, T_INET_1, and T_INET_0.
? There is no SLA criteria configured for the health-check Level3_DNS. This means that the health check does not use any SLA parameters to determine the state of the interface2. In the exhibit, the sla map value is 0x0 for both port1 and port2, indicating that no SLA criteria are applied.

NEW QUESTION 6
Which two statements about SD-WAN central management are true? (Choose two.)

A. It does not allow you to monitor the status of SD-WAN members.
B. It is enabled or disabled on a per-ADOM basis.
C. It is enabled by default.
D. It uses templates to configure SD-WAN on managed devices.

Answer: BD

NEW QUESTION 7
What does enabling the exchange-interface-ip setting enable FortiGate devices to exchange?

A. The gateway address of their IPsec interfaces
B. The tunnel ID of their IPsec interfaces
C. The IP address of their IPsec interfaces
D. The name of their IPsec interfaces

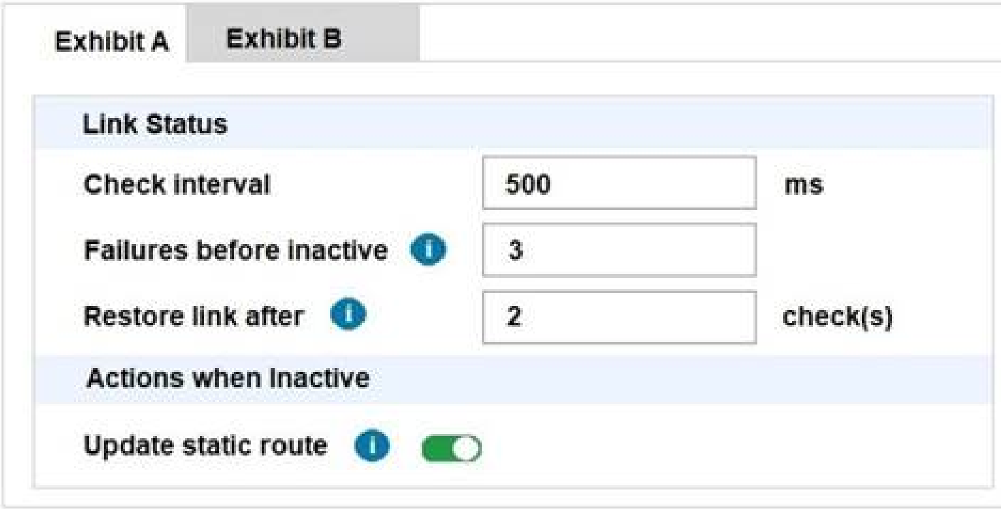
Answer: C

NEW QUESTION 8
What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

A. FEC supports hardware offloading.
B. FEC improves reliability of noisy links.
C. FEC transmits parity packets that can be used to reconstruct packet loss.
D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 9
Refer to the Exhibits:



Link Status

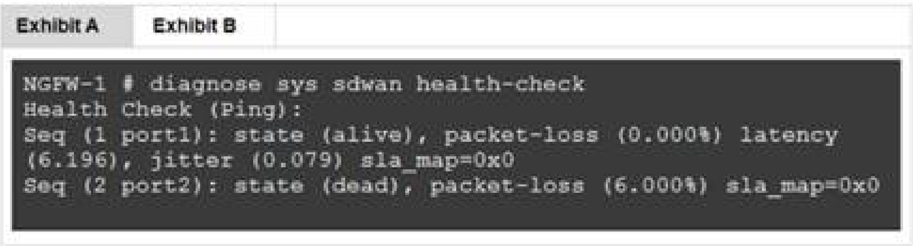
Check interval 500 ms

Failures before inactive 3

Restore link after 2 check(s)

Actions when Inactive

Update static route (enabled)



```
NGFW-1 # diagnose sys sdwan health-check
Health Check (Ping):
Seq (1 port1): state (alive), packet-loss (0.000%) latency
(6.196), jitter (0.079) sla_map=0x0
Seq (2 port2): state (dead), packet-loss (6.000%) sla_map=0x0
```

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members.
Based on the exhibits, which statement is correct?

A. The dead member interface stays unavailable until an administrator manually brings the interface back.
B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
C. Static routes using port2 are active in the routing table.
D. FortiGate has not received three consecutive requests from the SLA server configured for port2.

Answer: C

NEW QUESTION 10
Which statement about SD-WAN zones is true?

A. An SD-WAN zone can contain only one type of interface.
B. An SD-WAN zone can contain between 0 and 512 members.
C. You cannot use an SD-WAN zone in static route definitions.
D. You can configure up to 32 SD-WAN zones per VDOM.

Answer: D

Explanation:
SD-WAN zones are a group of interfaces that share the same SD-WAN settings, such as health check, SLA, and load balancing. Some characteristics of SD-WAN zones are:
? An SD-WAN zone can contain different types of interfaces, such as physical, VLAN, aggregate, and tunnel interfaces1.
? An SD-WAN zone can contain up to 512 members1.
? You can use an SD-WAN zone in static route definitions, as long as the destination interface is also an SD-WAN zone1.
? You can configure up to 32 SD-WAN zones per VDOM1.

NEW QUESTION 10
Refer to the exhibit.

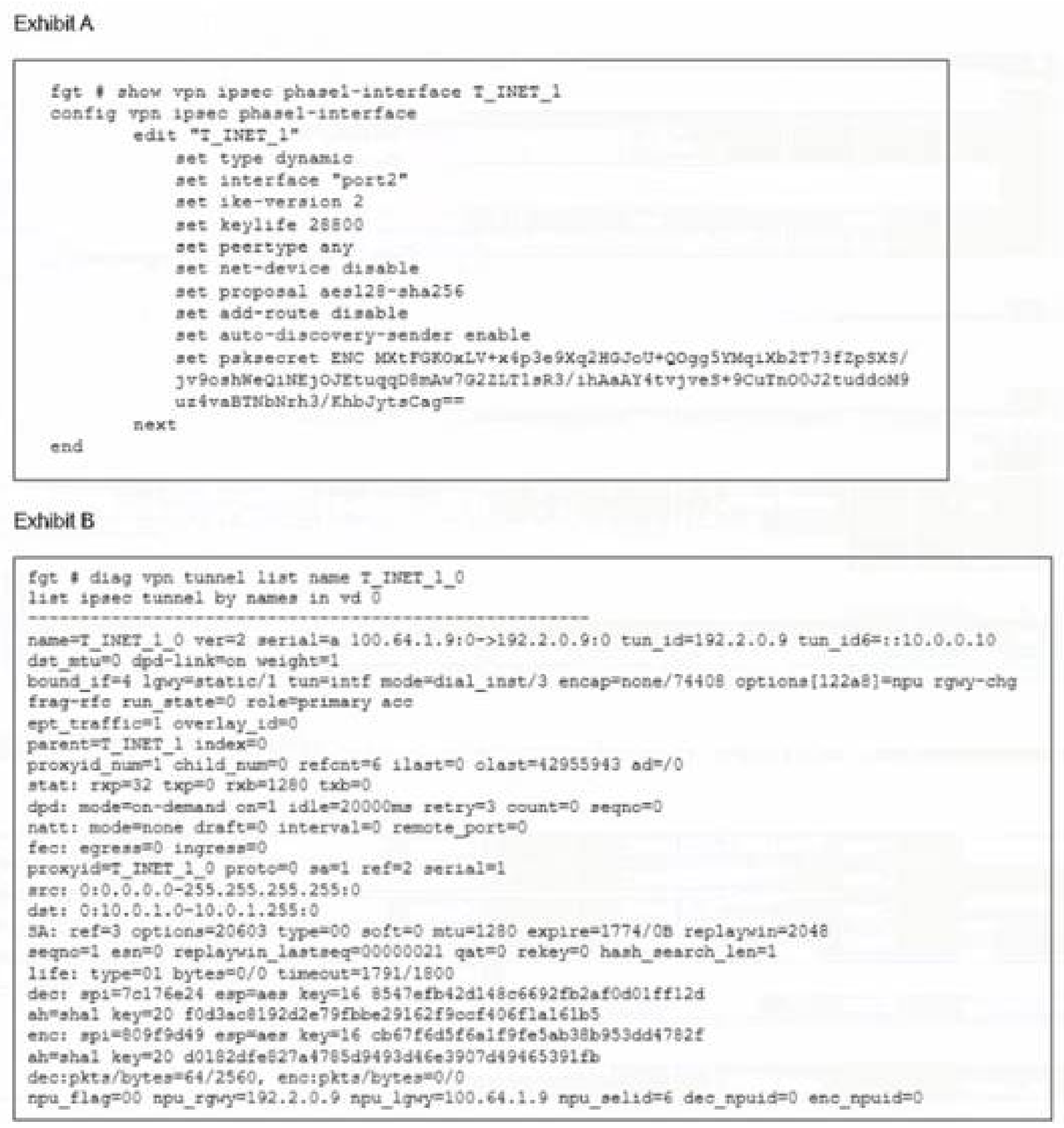


Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
        edit "T_INET_1"
            set type dynamic
            set interface "port2"
            set ike-version 2
            set keylife 28800
            set peertype any
            set net-device disable
            set proposal aes128-sha256
            set add-route disable
            set auto-discovery-sender enable
            set psksecret ENC MXtFGKOxLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73fZpSXS/
            jv9oshWeQiNEjOJEtuqqD8mAw7G2ZLT1sR3/ihAaAY4tvjveS+9CuTnO0J2tuddoM9
            uz4vaBTNbNrh3/KhbJytsCag==
        next
end
```

Exhibit B

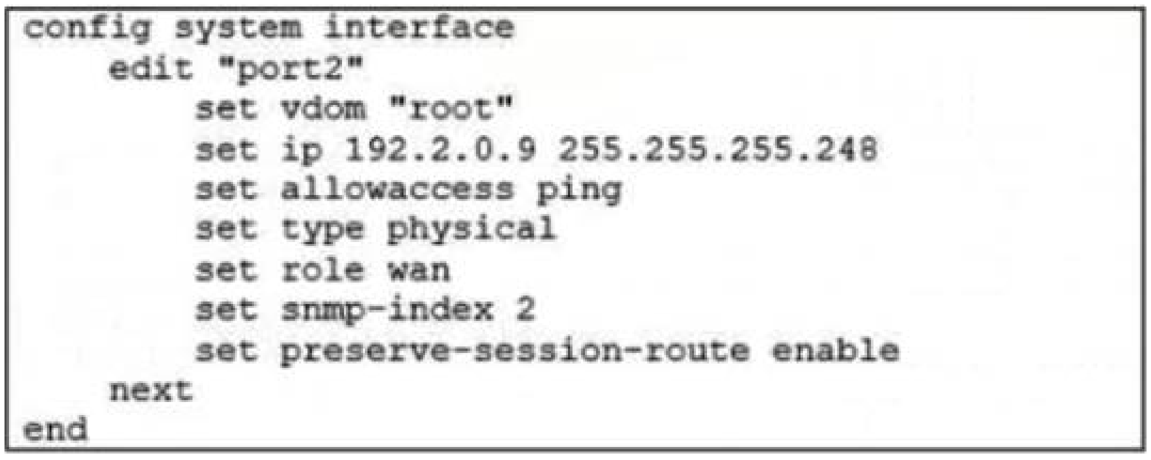
```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=::10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag-rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=42955943 ad=/0
stat: rxp=32 txp=0 rxb=1280 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
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=sha1 key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6a1f9fe5ab38b953dd4782f
ah=sha1 key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_lgwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=0
```

Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

A. FortiGate does not install IPsec static routes for remote protected networks in the routing tabl
B. Most Voted
C. The phase 1 configuration supports the network-overlay settin
D. Most Voted
E. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
F. Dead peer detection is disabled.

Answer: AC

NEW QUESTION 14
Refer to the exhibit.



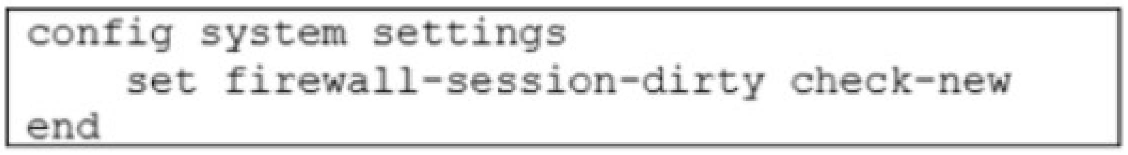
```
config system interface
    edit "port2"
        set vdom "root"
        set ip 192.2.0.9 255.255.255.248
        set allowaccess ping
        set type physical
        set role wan
        set snmp-index 2
        set preserve-session-route enable
    next
end
```

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)

A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.
B. FortiGate performs routing lookups for new sessions only, after a route change.
C. FortiGate always blocks all traffic, after a route change.
D. FortiGate flushes all routing information from the session table, after a route change.

Answer: AB

NEW QUESTION 19
Refer to the exhibit.



```
config system settings
    set firewall-session-dirty check-new
end
```

Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

A. FortiGate flushes all sessions.
B. FortiGate terminates the old sessions.

C. FortiGate does not change existing sessions.
D. FortiGate evaluates new sessions.

Answer: CD

Explanation:
FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new. The results is that FortiGate evaluates only new session against the new firewall policy.

NEW QUESTION 24
Refer to the exhibits.

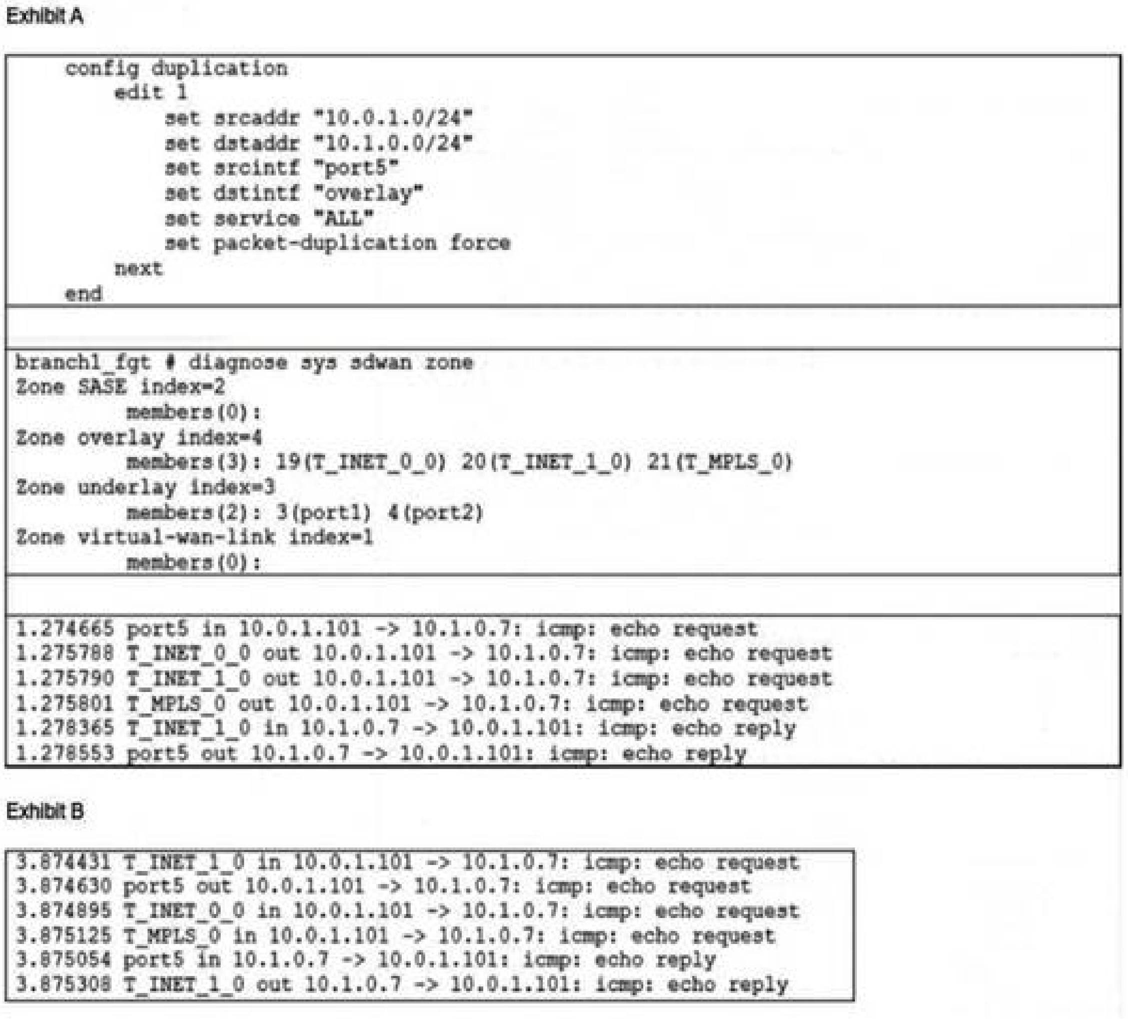


Exhibit A

```
    config duplication
        edit 1
            set srcaddr "10.0.1.0/24"
            set dstaddr "10.1.0.0/24"
            set srcintf "port5"
            set dstintf "overlay"
            set service "ALL"
            set packet-duplication force
        next
    end
```

```
branch1_fgt # diagnose sys sdwan zone
Zone SASE index=2
         members(0):
Zone overlay index=4
         members(3): 19(T_INET_0_0) 20(T_INET_1_0) 21(T_MPLS_0)
Zone underlay index=3
         members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
         members(0):
```

```
1.274665 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275788 T_INET_0_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275790 T_INET_1_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275801 T_MPLS_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.278365 T_INET_1_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.278553 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

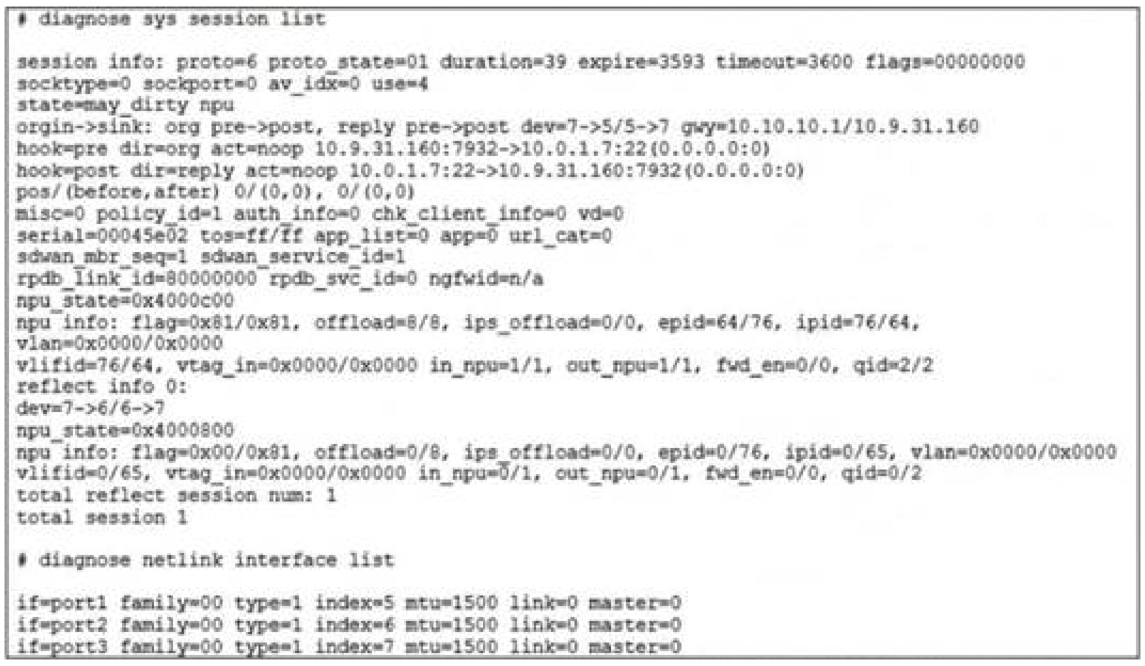
```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.875308 T_INET_1_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on FortiGate acting as the sender. Exhibit B shows the sniffer output on a FortiGate acting as the receiver.
The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T_INET_1_0.
Based on the output shown in the exhibits, which two reasons can cause the observed behavior? (Choose two.)

A. On the receiver FortiGate, packet-de-duplication is enabled.
B. The ICMP echo request packets sent over T_INET_0_0 and T_MPLS_0 were dropped along the way.
C. The ICMP echo request packets received over T_INET_0_0 and T_MPLS_0 were offloaded to NPU.
D. On the sender FortiGate, duplication-max-num is set to 3.

Answer: AD

NEW QUESTION 26
Refer to the exhibit.



```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=39 expire=3593 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
state=may_dirty npu
orgin->sink: org pre->post, reply pre->post dev=7->5/5->7 gwy=10.10.10.1/10.9.31.160
hook=pre dir=org act=noop 10.9.31.160:7932->10.0.1.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.0.1.7:22->10.9.31.160:7932(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=00045e02 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x4000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/76, ipid=76/64,
vlan=0x0000/0x0000
vlifid=76/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/2
reflect info 0:
dev=7->6/6->7
npu_state=0x4000800
npu info: flag=0x00/0x81, offload=0/8, ips_offload=0/0, epid=0/76, ipid=0/65, vlan=0x0000/0x0000
vlifid=0/65, vtag_in=0x0000/0x0000 in_npu=0/1, out_npu=0/1, fwd_en=0/0, qid=0/2
total reflect session num: 1
total session 1

# diagnose netlink interface list

if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate appliance that supports hardware offloading. Based on the information shown in the exhibits, which two statements about the session are true? (Choose two.)

A. The reply direction of the asymmetric traffic flows from port2 to port3.
B. The auxiliary session can be offloaded to hardware.
C. The original direction of the symmetric traffic flows from port3 to port2.

D. The main session cannot be offloaded to hardware.

Answer: AB

NEW QUESTION 29
Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

A. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements
B. Member metrics are measured only if an SLA target is configured
C. When configuring an SD-WAN rule you can select multiple SLA targets of the same performance SLA
D. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy

Answer: AD

NEW QUESTION 31
What three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

A. You can apply a system template and a CLI template to the same FortiGate device.
B. A CLI template can be of type CLI script or Perl script.
C. A template group can include a system template and an SD-WAN template.
D. A template group can contain CLI templates of both types.
E. Templates are applied in order, from top to bottom.

Answer: BDE

Explanation:
According to the FortiManager Administration Guide, provisioning templates are used to configure FortiGate devices in a consistent and efficient way. There are different types of templates, such as system, IPsec, SD-WAN, certificate, and CLI templates. Some characteristics of provisioning templates are:
? You can apply a system template and a CLI template to the same FortiGate device, as long as they do not have conflicting settings1.
? A CLI template can be of type CLI script or Perl script. A CLI script template contains FortiOS CLI commands, while a Perl script template contains Perl code that can generate FortiOS CLI commands2.
? A template group can include a system template and an SD-WAN template, as well as other types of templates. A template group is a collection of templates that can be applied to multiple devices at once3.
? A template group can contain CLI templates of both types, as long as they do not have conflicting settings2.
? Templates are applied in order, from top to bottom. The order of the templates in a template group determines the order in which they are applied to the devices3.

NEW QUESTION 36
Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

A. http
B. icmp
C. twamp
D. dns

Answer: AD

Explanation:
Performance SLA (Service Level Agreement) protocols are used in SD-WAN to monitor the quality and performance of various network services. The two protocols that specifically allow for verifying a specific value in the server response are:
? HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It allows for fetching resources, such as HTML documents. You can configure an HTTP performance SLA to send specific requests (e.g., GET or POST) and then check if the response body contains a particular string or value. This is useful for validating web server functionality and content delivery.
? DNS (Domain Name System): DNS is responsible for translating domain names into IP addresses. A DNS performance SLA can be set up to query a specific domain and verify that the returned IP address or other DNS record values match what is expected. This helps ensure proper name resolution and accessibility of resources.

NEW QUESTION 39
Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

A. When configuring an SD-WAN rule, you can select multiple SLA targets of the same performance SLA.
B. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements.
C. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy.
D. Member metrics are measured only if an SLA target is configured.

Answer: BD

NEW QUESTION 44
Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

A. diagnose sys sdwan zone
B. diagnose sys sdwan service
C. diagnose sys sdwan member
D. diagnose sys sdwan interface

Answer: C

NEW QUESTION 46
What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide direct internet access on spokes
B. Provide internet access through the hub
C. Centralize security inspection on the hub
D. Provide thorough inspection on spokes

Answer: BC

Explanation:
* B. Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.
* C. Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NEW QUESTION 47
Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

A. hold-down-time
B. link-down-failover
C. auto-discovery-shortcuts
D. idle-timeout

Answer: A

NEW QUESTION 50
What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

A. It ensures consistent settings between phase1 and phase2.
B. It guides the administrator to use Fortinet recommended settings.
C. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
D. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

Answer: AB

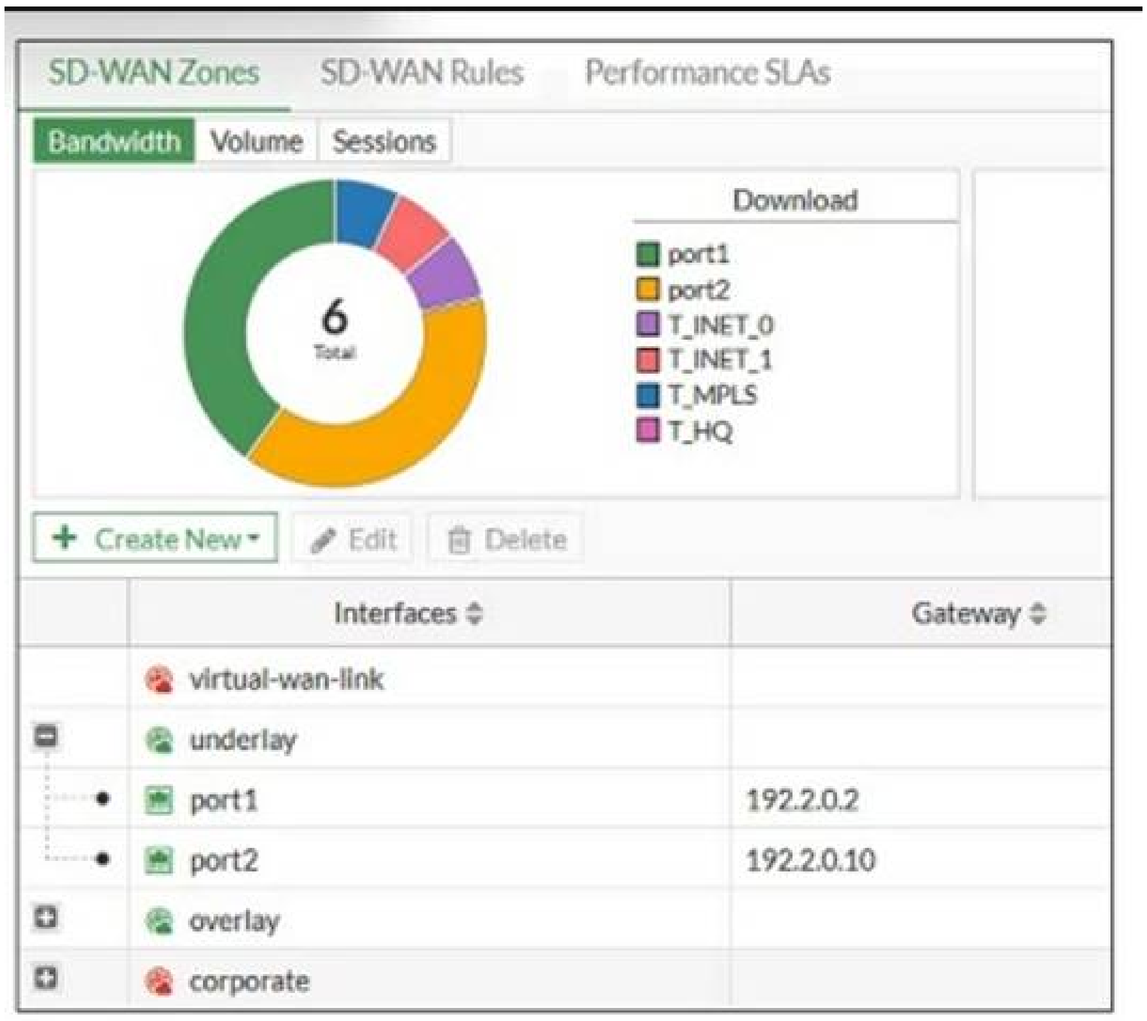
Explanation:
The use of an IPsec recommended template offers the advantage of ensuring consistent settings between phase1 and phase2 (A), which is essential for the stability and security of the IPsec tunnel. Additionally, it guides the administrator to use Fortinet's recommended settings (B), which are designed to optimize performance and security based on Fortinet's best practices. References: The benefits of using IPsec recommended templates are outlined in Fortinet's SD-WAN documentation, which emphasizes the importance of consistency and adherence to recommended configurations.

NEW QUESTION 52
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

A. Encapsulating Security Payload (ESP)
B. Secure Shell (SSH)
C. Internet Key Exchange (IKE)
D. Security Association (SA)

Answer: AC

NEW QUESTION 54
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



	Interfaces	Gateway
	virtual-wan-link	
⊟	underlay	
•	port1	192.2.0.2
•	port2	192.2.0.10
⊞	overlay	
⊞	corporate	

Based on the exhibit, which statement is true?

A. You can delete the virtual-wan-link zone because it contains no member.
B. The corporate zone contains no member.
C. You can move port1 from the underlay zone to the overlay zone.
D. The overlay zone contains four members.

Answer: B

Explanation:
Based on the exhibit, the "corporate" zone contains no member (B). In the FortiGate GUI, zones without members do not display any interfaces listed under them, which is the case for the corporate zone in the exhibit. References: This conclusion is based on standard Fortinet GUI interpretation and the operational logic of SD-WAN zones as per Fortinet's guidelines and user interface standards.

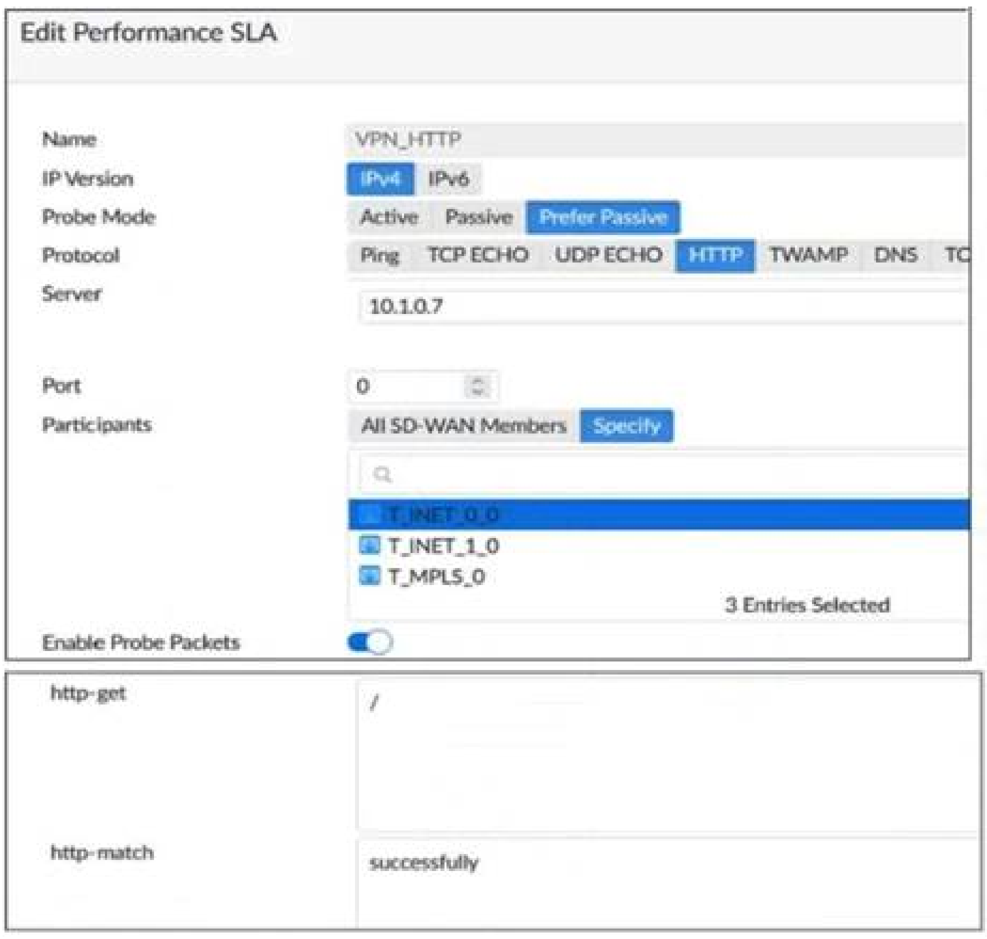
NEW QUESTION 58
Which two statements are correct when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The sdwan_service_id flag in the session information is 0.
B. All SD-WAN rules have the default setting enabled.
C. Traffic does not match any of the entries in the policy route table.
D. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

Answer: AC

Explanation:
sdwan_service_id is 0 = match SD-WAN implicit rule, study guide 7.0 page 120, 7.2 page 149 SD-WAN rules internally are interpreted as a Policy route, so when the traffic doesn't match with any policy route, it will be flowing by implicit policy.

NEW QUESTION 61
Refer to the exhibit.



Edit Performance SLA

Name: VPN_HTTP

IP Version: IPv4 | IPv6 (IPv4 selected)

Probe Mode: Active | Passive | Prefer Passive (Prefer Passive selected)

Protocol: Ping | TCP ECHO | UDP ECHO | HTTP | TWAMP | DNS | TC (HTTP selected)

Server: 10.1.0.7

Port: 0

Participants: All SD-WAN Members | Specify (Specify selected)

T_INET_0_0
T_INET_1_0
T_MPLS_0

3 Entries Selected

Enable Probe Packets: on

http-get: /

http-match: successfully

Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

A. After FortiGate switches to active mode, FortiGate never fails back to passive monitoring.
B. During passive monitoring, FortiGate can’t detect dead members.
C. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
D. FortiGate passively monitors the member if TCP traffic is passing through the member.

Answer: BD

NEW QUESTION 62
Refer to the exhibits. Exhibit A -

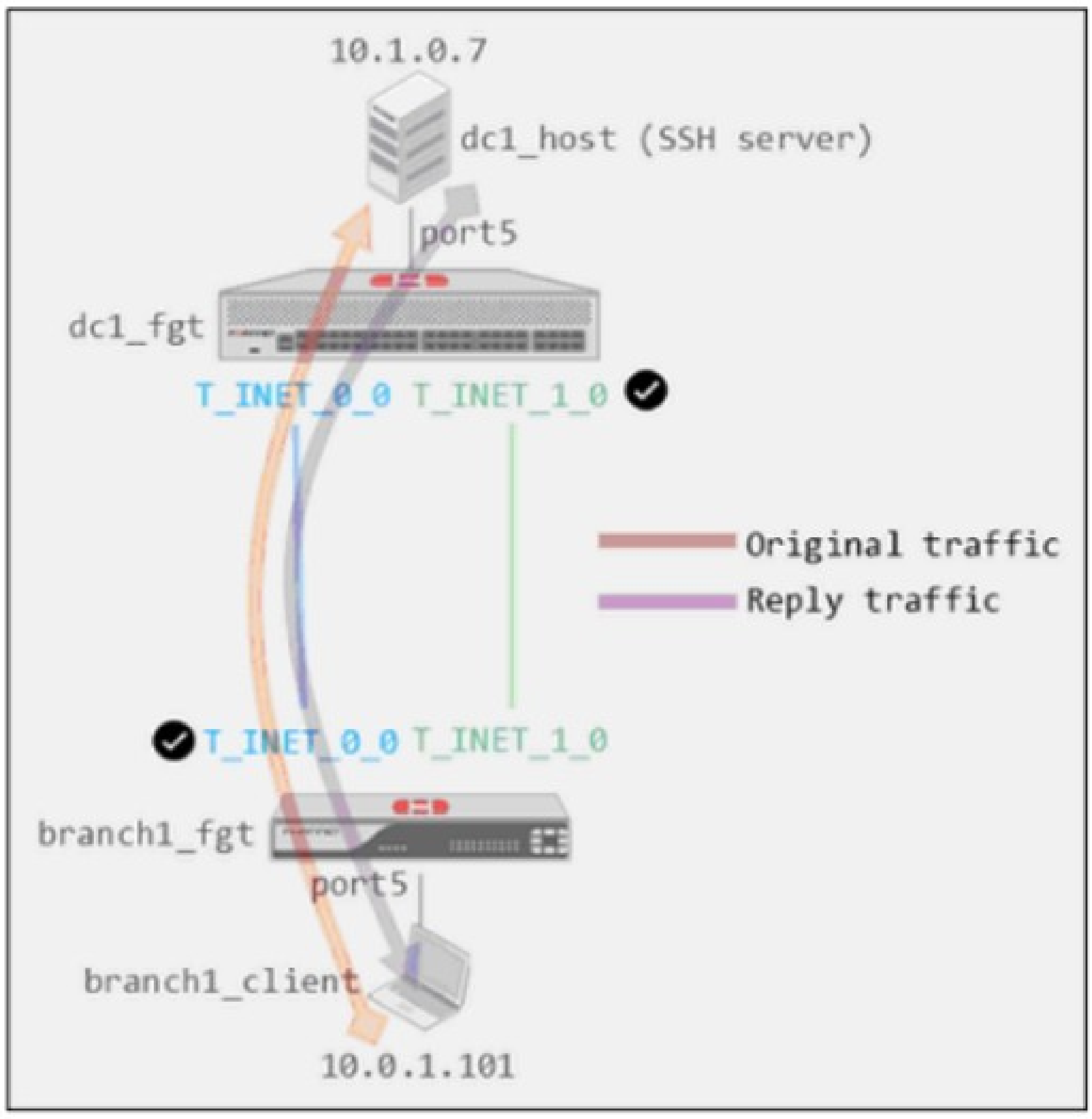
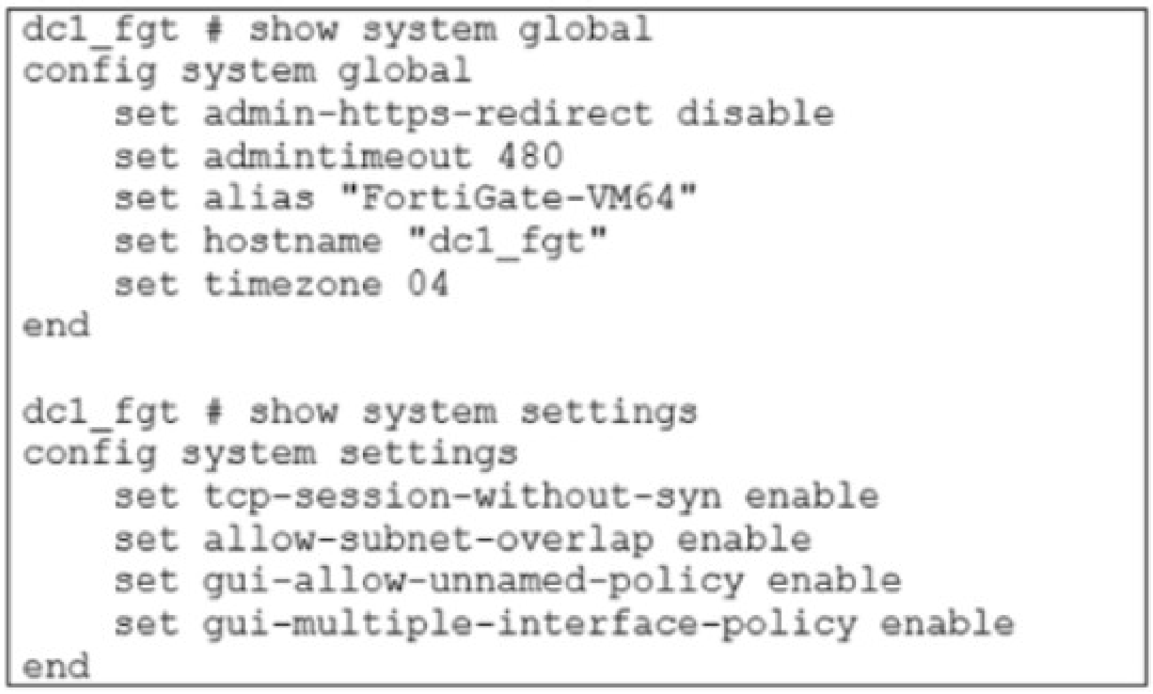


Exhibit B -



```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt.

When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

A. Enable auxiliary-session under config system settings.
B. Disable tp-session-without-syn under config system settings.
C. Enable snat-route-change under config system global.
D. Disable allow-subnet-overlap under config system settings.

Answer: A

NEW QUESTION 63
Which two statements describe how IPsec phase 1 main mode id different from aggressive mode when performing IKE negotiation? (Choose two.)

A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
B. XAuth is enabled as an additional level of authentication, which requires a username and password.
C. Three packets are exchanged between an initiator and a responder instead of six packets.
D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

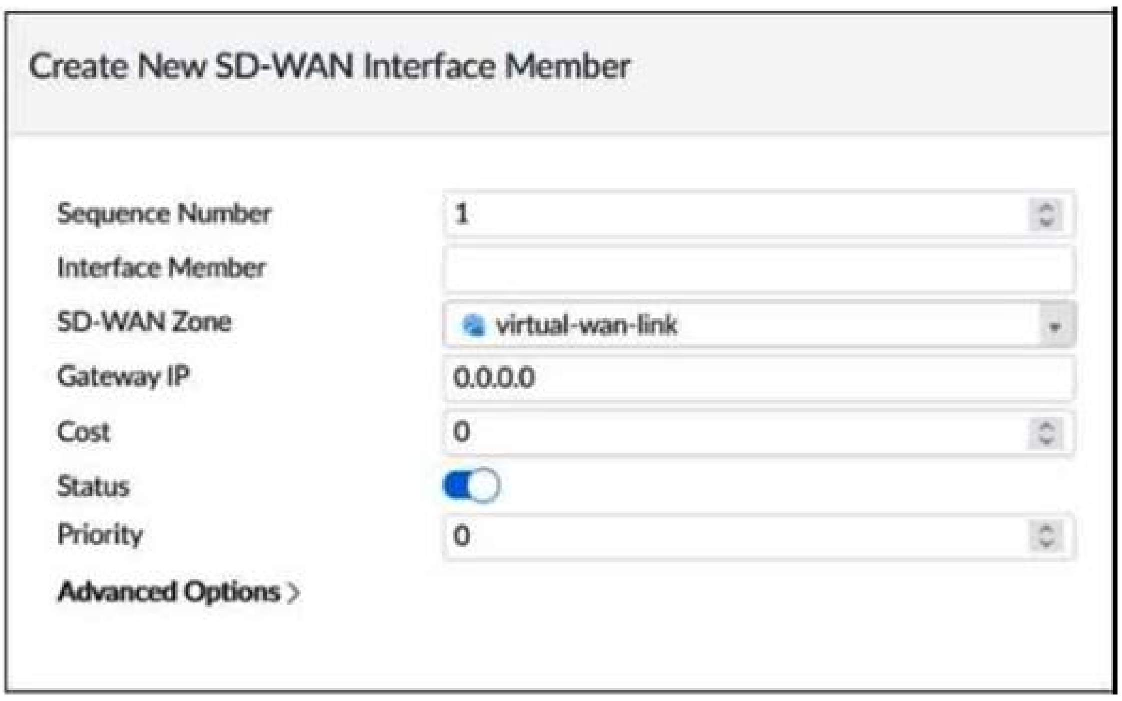
Answer: AC

NEW QUESTION 67
What is the route-tag setting in an SD-WAN rule used for?

A. To indicate the routes for health check probes.
B. To indicate the destination of a rule based on learned BGP prefixes.
C. To indicate the routes that can be used for routing SD-WAN traffic.
D. To indicate the members that can be used to route SD-WAN traffic.

Answer: B

NEW QUESTION 70
Refer to the exhibit.



Create New SD-WAN Interface Member

Sequence Number	1
Interface Member	
SD-WAN Zone	virtual-wan-link
Gateway IP	0.0.0.0
Cost	0
Status	●
Priority	0

Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)

A. Cost
B. Interface member
C. Priority

D. Gateway IP

Answer: BD

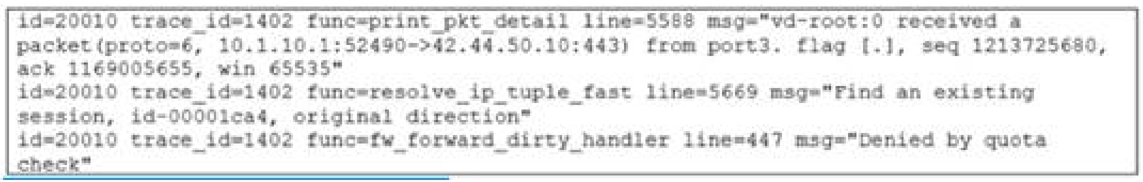
NEW QUESTION 71
The administrator uses the FortiManager SD-WAN overlay template to prepare an SD- WAN deployment. With information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on spoke and hub devices.
Select three templates created by the SD-WAN overlay template for a spoke device. (Choose three.)

A. System template
B. BGP template
C. IPsec tunnel template
D. CLI template
E. Overlay template

Answer: ACE

Explanation:
In a FortiManager SD-WAN overlay template configuration for a spoke device, the system template (A) is created to provide basic device settings. The IPsec tunnel template (C) is generated to establish secure tunnels between the spoke and the hub devices. Lastly, the overlay template (E) is configured to specify the overlay network settings, which often include the SD-WAN rules and performance SLAs.

NEW QUESTION 74
Exhibit.



```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.], seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

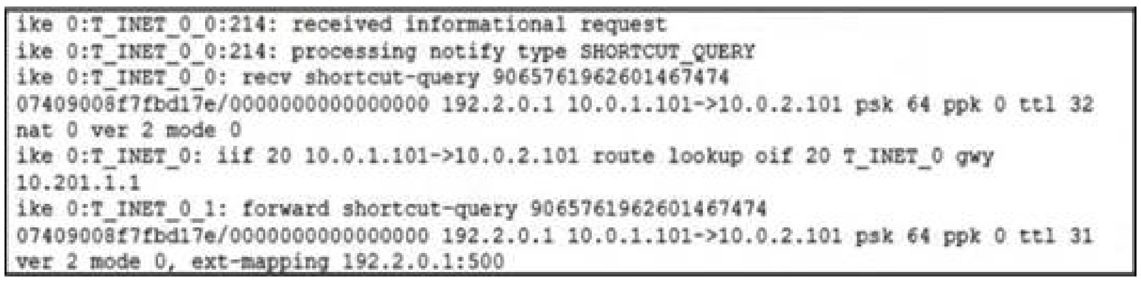
Which conclusion about the packet debug flow output is correct?

A. The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
B. The packet size exceeded the outgoing interface MTU.
C. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
D. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.

Answer: C

Explanation:
In a Per-IP shaper configuration, if an IP address exceeds the configured concurrent session limit, the message "Denied by quota check" appears. SD-WAN 7.0 Study Guide page 287

NEW QUESTION 76
Refer to the exhibit.



```
ike 0:T_INET_0_0:214: received informational request
ike 0:T_INET_0_0:214: processing notify type SHORTCUT_QUERY
ike 0:T_INET_0_0: recv shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 32
nat 0 ver 2 mode 0
ike 0:T_INET_0: iif 20 10.0.1.101->10.0.2.101 route lookup oif 20 T_INET_0 gwy
10.201.1.1
ike 0:T_INET_0_1: forward shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 31
ver 2 mode 0, ext-mapping 192.2.0.1:500
```

Which statement about the role of the ADVPN device in handling traffic is true?

A. This is a spoke that has received a query from a remote hub and has forwarded the response to its hub.
B. Two hubs, 10.0.1.101 and 10.0.2.101, are receiving and forwarding queries between each other.
C. This is a hub that has received a query from a spoke and has forwarded it to another spoke.
D. Two spokes, 192.2.0.1 and 10.0.2.101, forward their queries to their hubs.

Answer: C

NEW QUESTION 81
Which statement is correct about SD-WAN and ADVPN?

A. Routes for ADVPN shortcuts must be manually configured.
B. SD-WAN can steer traffic to ADVPN shortcuts, established over IPsec overlays, configured as SD-WAN members.
C. SD-WAN does not monitor the health and performance of ADVPN shortcuts.
D. You must use IKEv2 on IPsec tunnels.

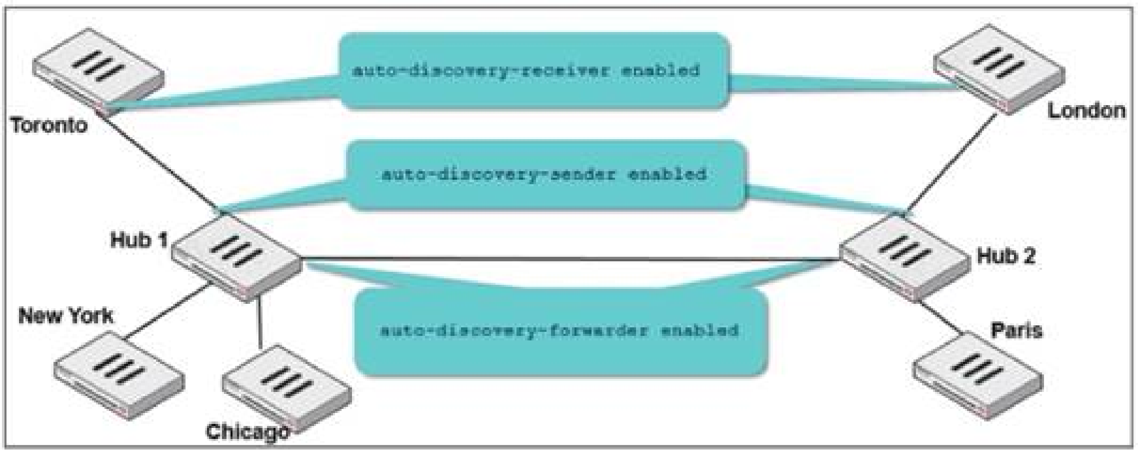
Answer: B

NEW QUESTION 84
Which statement about using BGP routes in SD-WAN is true?

A. Learned routes can be used as dynamic destinations in SD-WAN rules.
B. You must use BGP to route traffic for both overlay and underlay links.
C. You must configure AS path prepending.
D. You must use external BGP.

Answer: A

NEW QUESTION 87
Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. The administrator configured ADVPN on both hub-and-spoke groups.\

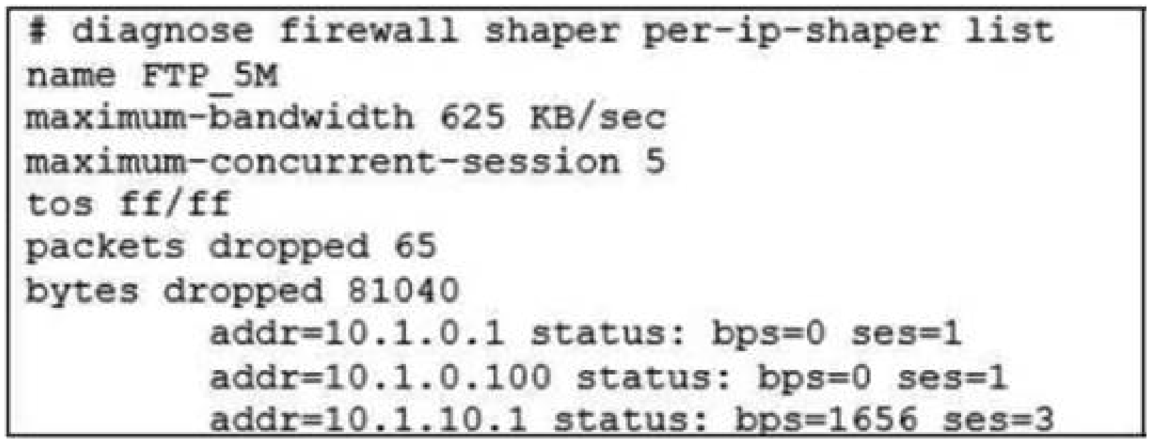

auto-discovery-receiver enabled
Toronto
London
auto-discovery-sender enabled
Hub 1
Hub 2
New York
auto-discovery-forwarder enabled
Paris
Chicago

Which two outcomes are expected if a user in Toronto sends traffic to London? (Choose two.)

A. London generates an IKE information message that contains the Toronto public IP address.
B. Traffic from Toronto to London triggers the dynamic negotiation of a direct site-to-site VPN.
C. Toronto needs to establish a site-to-site tunnel with Hub 2 to bypass Hub 1.
D. The first packets from Toronto to London are routed through Hub 1 then to Hub 2.

Answer: BD

NEW QUESTION 92
Refer to the exhibit.



```
# diagnose firewall shaper per-ip-shaper list
name FTP_5M
maximum-bandwidth 625 KB/sec
maximum-concurrent-session 5
tos ff/ff
packets dropped 65
bytes dropped 81040
        addr=10.1.0.1 status: bps=0 ses=1
        addr=10.1.0.100 status: bps=0 ses=1
        addr=10.1.10.1 status: bps=1656 ses=3
```

Which are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 94
......