Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

NEW QUESTION 1
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 2
Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

A. diagnose sys sdwan intf-sla-log
B. diagnose sys sdwan health-check
C. diagnose sys sdwan log
D. diagnose sys sdwan sla-log

Answer: D

Explanation:
SD-WAN 7.2 Study Guide page 321 You can view the stored member metrics by running the diagnose sys sdwan sla-log command. Note that you must include the name of the performance SLA followed by the member configuration index number. To display the SLA logs per interface, you run the diagnose sys sdwan intf-sla-log command.

NEW QUESTION 3
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 4
Refer to the exhibit.

```
config system virtual-wan-link
    set status enable
    set load-balance-mode source-ip-based
    config members
        edit 1
                set interface "port1"
                set gateway 100.64.1.254
                set source 100.64.1.1
                set cost 15
        next
        edit 2
                set interface "port2"
                set gateway 100.64.2.254
                set priority 10
        next
    end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

A. Set priority 10.
B. Set cost 15.
C. Set load-balance-mode source-ip-ip-based.
D. Set source 100.64.1.1.

Answer: AB

NEW QUESTION 5
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 6
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 7
What is a benefit of using application steering in SD-WAN?

A. The traffic always skips the regular policy routes.
B. You steer traffic based on the detected application.
C. You do not need to enable SSL inspection.

D. You do not need to configure firewall policies that accept the SD-WAN traffic.

Answer: B

NEW QUESTION 8
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: BC

NEW QUESTION 9
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 implict policy.

NEW QUESTION 10
Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

A. Interface-based shaping mode
B. Reverse-policy shaping mode
C. Shared-policy shaping mode
D. Per-IP shaping mode

Answer: A

Explanation:
Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

NEW QUESTION 10
Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

A. update-source
B. set-route-tag
C. holdtime-timer
D. link-down-failover

Answer: CD

NEW QUESTION 11
Refer to the exhibit.

```
session info: proto=6 proto_state=11 duration=242 expire=3349 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:34676->128.66.0.1:22(192.2.0.1:34676)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:34676(10.0.1.101:34676)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:34676(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008
```

Which statement explains the output shown in the exhibit?

A. FortiGate performed standard FIB routing on the session.
B. FortiGate will not re-evaluate the session following a firewall policy change.
C. FortiGate used 192.2.0.1 as the gateway for the original direction of the traffic.

D. FortiGate must re-evaluate the session due to routing change.

Answer: D

NEW QUESTION 13
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: AD

NEW QUESTION 15
Refer to the exhibits.
Exhibit A

Edit Performance SLA

Name	Level3_DNS
IP Version	**IPv4** IPv6
Probe Mode	**Active** Passive Prefer Passive
Protocol	**Ping** TCP ECHO UDP ECHO HTTP TW/
Server	4.2.2.1
	4.2.2.2
Participants	All SD-WAN Members **Specify**
	🔍
	port1
	port2
	2 Entries
Enable Probe Packets	🔵

SLA Targets ⓘ

+ Add Target

Link Status

Interval	500 ⌄	Milliseconds
Failure Before Inactive	3 ⌄	(max 3600)
Restore Link After	2 ⌄	(max 3600)

Action When Inactive

Update Static Route	🔵
Cascade Interfaces	🔵

Exhibit B

```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0


branch1_fgt # get router info routing-table all | grep port
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
                  [1/0] via 192.2.0.10, port2
S       8.8.8.8/32 [10/0] via 192.2.0.11, port2
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10


branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status.
If port2 is detected dead by FortiGate, what is the expected behavior?

A. Port2 becomes alive after three successful probes are detected.
B. FortiGate removes all static routes for port2.
C. The administrator manually restores the static routes for port2, if port2 becomes alive.
D. Host 8.8.8.8 is reachable through port1 and port2.

Answer: B

Explanation:
This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

NEW QUESTION 18
Which two statements about the SD-WAN zone configuration are true? (Choose two.)

A. The service-sla-tie-break setting enables you to configure preferred member selection based on the best route to the destination.
B. You can delete the default zones.
C. The default zones are virtual-wan-link and SASE.
D. An SD-WAN member can belong to two or more zones.

Answer: AC

NEW QUESTION 22
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
    2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
    3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, 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 (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set priority-members 3 4 5
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

A. When T_INET_0_0 and T_MPLS_0 have the same latency.
B. When T_MPLS_0 has a latency of 100 ms.
C. When T_INET_0_0 has a latency of 250 ms.
D. When T_N1PLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 25
Refer to the exhibit.

```
config system sdwan
    set status enable
    set load-balance source-dest-ip-based
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
        edit "underlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 192.2.0.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 192.2.0.10
        next
    end
...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. All traffic from a source IP is sent to the same interface.
C. All traffic from a source IP is sent to the most used interface.
D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

NEW QUESTION 30
Refer to the exhibit.

```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Level3_DNS"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            set members 3
        next
    end
end
```

Based on the exhibit, which action does FortiGate take?

A. FortiGate bounces port5 after it detects all SD-WAN members as dead.
B. FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.
C. FortiGate brings up port5 after it detects all SD-WAN members as alive.
D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: B

NEW QUESTION 31
Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
B. The measured bandwidth is less than 100 KBps.
C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

Answer: BC

NEW QUESTION 35
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.
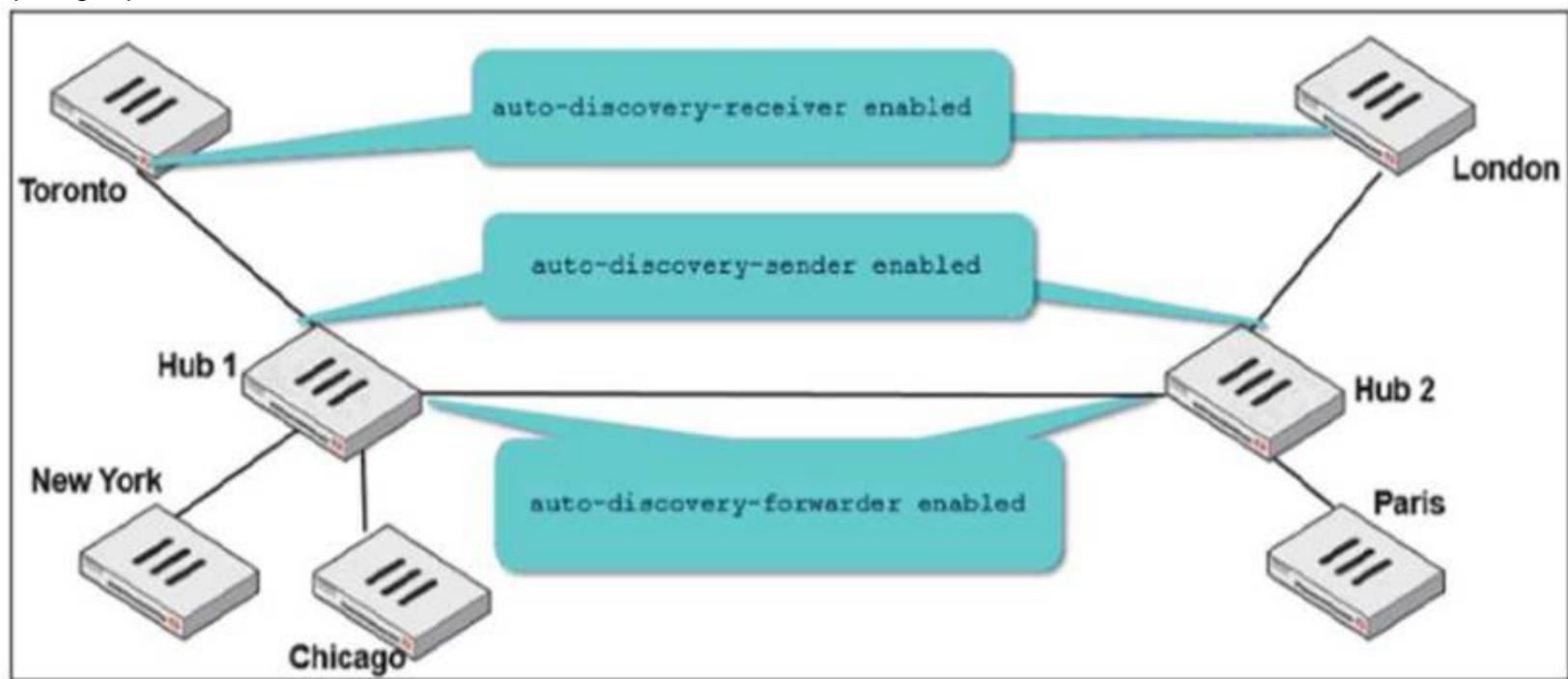
Which two outcomes are expected if a user in Toronto sends traffic to London? (Choose two.)

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 38
Which two tasks are part of using central VPN management? (Choose two.)

A. You can configure full mesh, star, and dial-up VPN topologies.
B. You must enable VPN zones for SD-WAN deployments.
C. FortiManager installs VPN settings on both managed and external gateways.
D. You configure VPN communities to define common IPsec settings shared by all VPN gateways.

Answer: AD

NEW QUESTION 43
Refer to the exhibit.

```
config firewall policy
    edit 1
        set anti-replay disable
    next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti-replay setting on the hubs?

A. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.
B. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the

hubs.
C. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.
D. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

Answer: B

NEW QUESTION 47
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 51
Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

A. Type of physical link connection
B. Internet service database (ISDB) address object
C. Source and destination IP address
D. URL categories
E. Application signatures

Answer: BCE

NEW QUESTION 52
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
origin->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 57
Refer to the exhibits. Exhibit A

```
branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode sla
        set dst "Corp-net"
        set src "LAN-net"
        config sla
            edit "VPN_PING"
                set id 1
            next
            edit "VPN_HTTP"
                set id 1
            next
        end
        set priority-members 3 4 5
        set gateway enable
    next
end
```

Exhibit B

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
    2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), 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 # get router info routing-table all | grep T_
S       10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
                   [1/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S       10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5


branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1,  peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9,  peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4 , gateway: 172.16.1.5,  peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.
The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

A. The traffic will be load balanced across all three overlays.
B. The traffic will be routed over T_INET_0_0.
C. The traffic will be routed over T_MPLS_0.
D. The traffic will be routed over T_INET_1_0.

Answer: D

NEW QUESTION 62
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 64
Refer to the exhibits.
Exhibit A
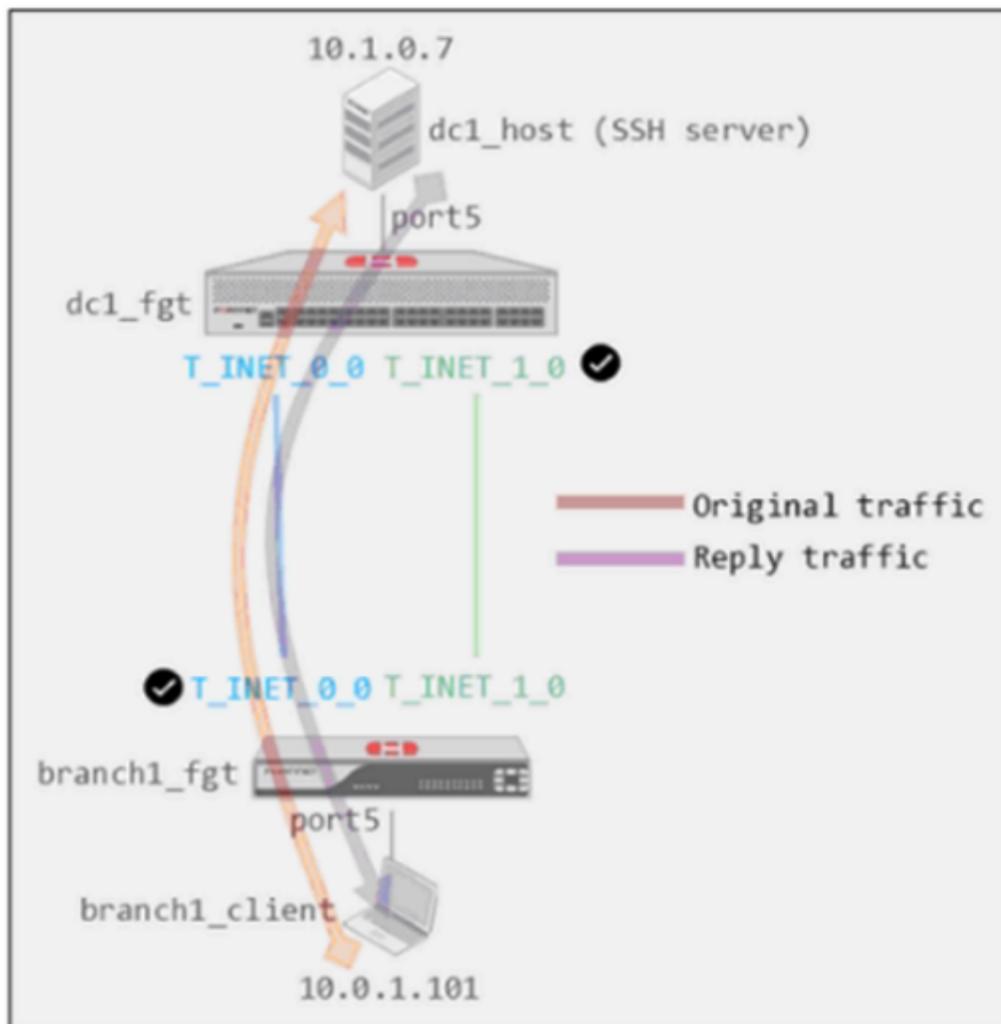
Exhibit B

```
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

Explanation:
Controlling return path with auxiliary session When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. Auxiliary sessions can be used to handle these changes to traffic patterns.https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/14295/controlling-return-path

NEW QUESTION 69
Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)

A. FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.
B. By default, local-out traffic does not use SD-WAN.
C. By default, FortiGate does not check if the selected member has a valid route to the destination.
D. You must configure each local-out feature individually, to use SD-WAN.

Answer: BD

NEW QUESTION 74
Refer to the exhibit.
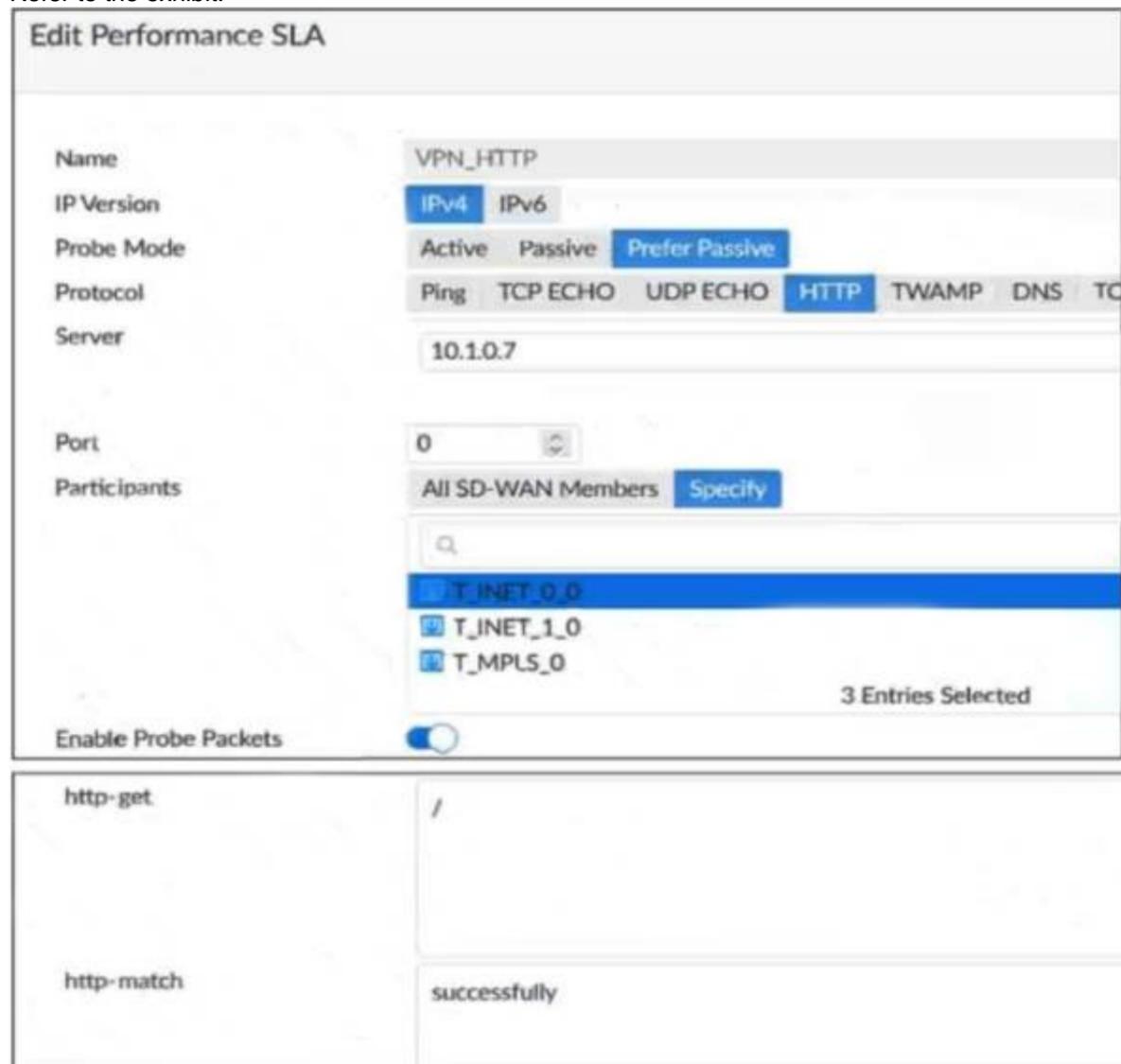
Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

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 77
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

Money Back Guarantee

NSE7_SDW-7.0 Practice Exam Features:

* NSE7_SDW-7.0 Questions and Answers Updated Frequently

* NSE7_SDW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_SDW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year