NSE7_SDW-7.0 Dumps

Fortinet NSE 7 - SD-WAN 7.0

https://www.certleader.com/NSE7_SDW-7.0-dumps.html

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.
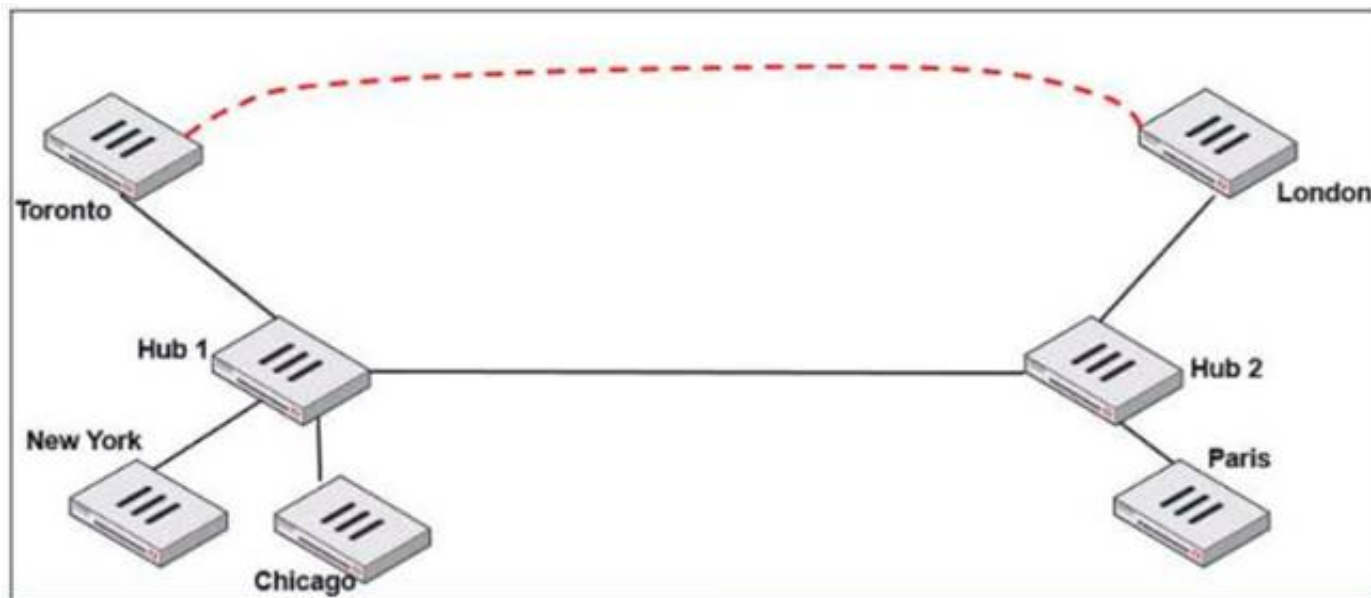
Answer: AD

NEW QUESTION 2
In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
B. It provides direct connectivity between spokes by creating shortcuts.
C. It enables spokes to bypass the hub during shortcut negotiation.
D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 3
Refer to the exhibit.

Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. Which two configuration settings are required for Toronto and London spokes to establish an ADVPN
shortcut? (Choose two.)

A. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
B. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
C. auto-discovery-forwarder must be enabled on all IPsec VPNs.
D. On the hubs, net-device must be enabled on all IPsec VPNs.

Answer: AB

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
Which two statements describe how IPsec phase 1 main mode is 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. A total of six packets are exchanged between an initiator and a responder instead of three packets.
D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: BC

NEW QUESTION 6
Exhibit A –

#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
▼ Physical (10)						
1	port1	Physical	port1	Manual	203.0.113.1/255.255.255.2	PING
2	port2	Physical	port2	Manual	203.0.113.9/255.255.255.2	PING
3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
4	port4	Physical	port4	Manual	172.16.0.9/255.255.255.24	PING
5	port5	Physical	port5	Manual	10.0.2.254/255.255.255.0	PING
6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
10	port10	Physical	port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT
▼ Aggregate (1)						
11	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
▼ Tunnel (3)						
12	naf.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
13	l2t.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
14	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0	
▼ EMAC VLAN (1)						
15	vl_lan_ts	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
▼ SD-WAN Zone (2)						
16	virtual-wan-link	SD-WAN Zone				
17	SASE	SD-WAN Zone	SASE			

#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
▼ Static Route (2)								
1	1	0.0.0.0/0.0.0.0	203.0.113.2	port1	10	0	Enable	
2	2	0.0.0.0/0.0.0.0	203.0.113.10	port2	10	0	Enable	

Exhibit B –

#	Name	From	To	Source	Destination	Schedule	Service
1	Internet_Access	port5	port1	all	all	always	ALL
▼ Implicit (2-2 / Total: 1)							
2	Implicit Deny	any	any	all all	all all	always	ALL

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.
Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

A. port1 is assigned a manual IP address.
B. port1 is referenced in a firewall policy.
C. port2 is referenced in a static route.
D. port1 and port2 are not administratively down.

Answer: B

NEW QUESTION 7
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 8
Refer to the exhibits.
Exhibit A

```
Network Properties
    Service                        Critical-DIA
Identity
    Device ID                      FGVM01TM22000077
    Device Name                    branch1_fgt
Type
    Sub Type                       sdwan
    Type                           event
Alerts
    Level                          notice
General
    Log Description                SDWAN status
    Log ID                         0113022923
    Message                        Service prioritized by performance metric will be redirected in sequence order.
    Sequence Number                2,1
    Virtual Domain                 root
Others
    Date/Time                      23:57:29
    Destination End User ID        3
    Destination Endpoint ID        3
    Device Time                    2022-03-04 14:57:27
    Event Time                     1646434647595788893
    Event Type                     Service
    Metric                         latency
    Service ID                     1
    Time Stamp                     2022-03-04 23:57:29
    Time Zone                      -0800
    UEBA Endpoint ID               3
    UEBA User ID                   3
    logver                         700030237
```

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
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


config service
    edit 1
        set name "Critical-DIA"
        set mode priority
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16354 41468 16920
        set health-check "Level3_DNS"
        set priority-members 1 2
    next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
B. Port2 has the highest member priority.
C. Port2 has a lower latency than port1.
D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 9
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: A

NEW QUESTION 10
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 10
Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last_used=2022-03-25 10:58:12
```

Based on the output, which two conclusions are true? (Choose two.)

A. There is more than one SD-WAN rule configured.
B. The SD-WAN rules take precedence over regular policy routes.
C. The all_rules rule represents the implicit SD-WAN rule.
D. Entry 1(id=1) is a regular policy route.

Answer: AD

NEW QUESTION 15
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 16
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 18
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 19
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 20
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 23
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 25
Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.], seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg="Find an existing
session, id-000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg="exceeded shaper limit, drop"
```

Which conclusion about the packet debug flow output is correct?

A. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
C. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

Answer: D

NEW QUESTION 28
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

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Assigning-Priority-to-SD-WAN-Members-for-Defau

NEW QUESTION 33
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 38
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 39

......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_SDW-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_SDW-7.0-dumps.html