

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

<pre>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</pre>
<pre>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):</pre>
<pre>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</pre>

Exhibit B

<pre>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</pre>
--

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

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/000000000000000000 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/000000000000000000 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

Exhibit A –

+ Create New ▾ Edit Delete Where Used Collapse All Column Settings ▾ More ▾							
<input type="checkbox"/>	#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
<input type="checkbox"/>	▼ Physical (10)						
<input type="checkbox"/>	1	port1	Physical	port1	Manual	203.0.113.1/255.255.255.2	PING
<input type="checkbox"/>	2	port2	Physical	port2	Manual	203.0.113.9/255.255.255.2	PING
<input type="checkbox"/>	3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	4	port4	Physical	port4	Manual	172.16.0.9/255.255.255.24	PING
<input type="checkbox"/>	5	port5	Physical	port5	Manual	10.0.2.254/255.255.255.0	PING
<input type="checkbox"/>	6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	10	port10	Physical	port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT
<input type="checkbox"/>	▼ Aggregate (1)						
<input type="checkbox"/>	11	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
<input type="checkbox"/>	▼ Tunnel (3)						
<input type="checkbox"/>	12	na1.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	13	i2t.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	14	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	▼ EMAC VLAN (1)						
<input type="checkbox"/>	15	vl_lan_ts	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
<input type="checkbox"/>	▼ SD-WAN Zone (2)						
<input type="checkbox"/>	16	virtual-wan-link	SD-WAN Zone				
<input type="checkbox"/>	17	SASE	SD-WAN Zone	SASE			

+ Create New ▾ Edit Delete				Column Settings ▾					
<input type="checkbox"/>	#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
<input type="checkbox"/>	▼ Static Route (2)								
<input type="checkbox"/>	1	1	0.0.0.0/0.0.0.0	203.0.113.2	port1	10	0	Enable	
<input type="checkbox"/>	2	2	0.0.0.0/0.0.0.0	203.0.113.10	port2	10	0	Enable	

Exhibit B –

+ Create New	Edit	Delete	Section	Policy Lookup	Collapse All	Column Settings	View Mode	
#	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	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

Refer to the exhibit.

```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:2246->8.8.8.8:8 (192.168.73.132:62662)
hook=pre dir=reply act=dnat 8.8.8.8:62662->192.168.73.132:0 (10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

Based on the exhibit, which statement about FortiGate re-evaluating traffic is true?

- A. The type of traffic defined and allowed on firewall policy ID 1 is UDP.
- B. FortiGate has terminated the session after a change on policy ID 1.
- C. Changes have been made on firewall policy ID 1 on FortiGate.
- D. Firewall policy ID 1 has source NAT disabled.

Answer: C

NEW QUESTION 8

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 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

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1), alive, selected
    2: Seq_num(2 port2), alive, selected
  Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
  Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
  Src address(1):
    10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2), alive, selected
  Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838276,0,0,0 16001)
  Src address(1):
    10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*    0.0.0.0/0 [1/0] via 192.2.0.2, port1
      [1/0] via 192.2.0.10, port2
...
```


Exhibit B

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP: 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2		port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2		port2

Security	APP Count	2
Level	notice	
General	Log ID	0000000013
Session ID	769	
Tran Display	snat	
Virtual Domain	root	
Source	Country	Reserved
Device ID	FGVM01TM22000077	
Device Name	branch1_fgt	
IP	10.0.1.101	
Interface	port5	
Interface Role	undefined	
NAT IP	192.2.0.9	
NAT Port	51042	
Port	51042	
Source	10.0.1.101	
UEBA Endpoint ID	1025	
UEBA User ID	3	
Destination	Country	United States
End User ID	3	
Endpoint ID	101	
Host Name	www.gotomeeting.com	
IP	23.212.248.205	
Interface	port2	

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A. After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1. Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

- A. FortiGate did not refresh the routing information on the session after the application was detected.
- B. Port1 and port2 do not have a valid route to the destination.
- C. Full SSL inspection is not enabled on the matching firewall policy.
- D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

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 13

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "T_INET_0_0"
    set type dynamic
    set interface "port1"
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route enable
    set psksecret ENC
Zv9n4Urfk0W4jj8vWI+KywxBG4ZDT7jWHKd8YaL8jj4+pRpYOx/N7mSgc7VL0BW2ZHQUXWJ6zvFxnKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzqCGRYzLM8eFTOnK7K6Aux0bFDCpBBhEIdf+03CYBMLwkFZmdU6RsT+qvybblVX+Ioy
HK5EXakpmz5RiltELgZ9Gg==
  next
end
```

Which configuration change is required if the responder FortiGate uses a dynamic routing protocol to exchange routes over IPsec?

- A. type must be set to static.
- B. mode-cfg must be enabled.
- C. exchange-interface-ip must be enabled.
- D. add-route must be disabled.

Answer: D

Explanation:

for using "non ike" routes (for example BGP/static and so on) you must do disable the add-route that inject automatically kernel route based on p2 selectors from the remote site from the SD-WAN_7.2_Study_Guide page 236

NEW QUESTION 18

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 22

Refer to the exhibits. Exhibit A

```

config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077

```

Exhibit B

```

config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
    members(2): 3(port1) 4(port2)

```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

- A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
- B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
- C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
- D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: AD

Explanation:

Study Guide 7.0, pages 88 - 89.

Study Guide 7.2, pages 103 - 104.

Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

NEW QUESTION 24

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	<input checked="" type="checkbox"/>
Priority	0
Advanced Options >	

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 28

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 33

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 34

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 36

Which statement about using BGP for ADVPN is true?

- A. IBGP is preferred over EBGP, because IBGP preserves next hop information.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure BGP communities.
- D. You must configure AS path prepending.

Answer: A

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