

Fortinet

Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0



NEW QUESTION 1

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two)

- A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
- B. It improves SD-WAN performance on the managed FortiGate devices.
- C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
- D. It acts as a policy compliance entity to review all managed FortiGate devices.
- E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

NEW QUESTION 2

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 3

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 4

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(4294838278,0,0,0 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	

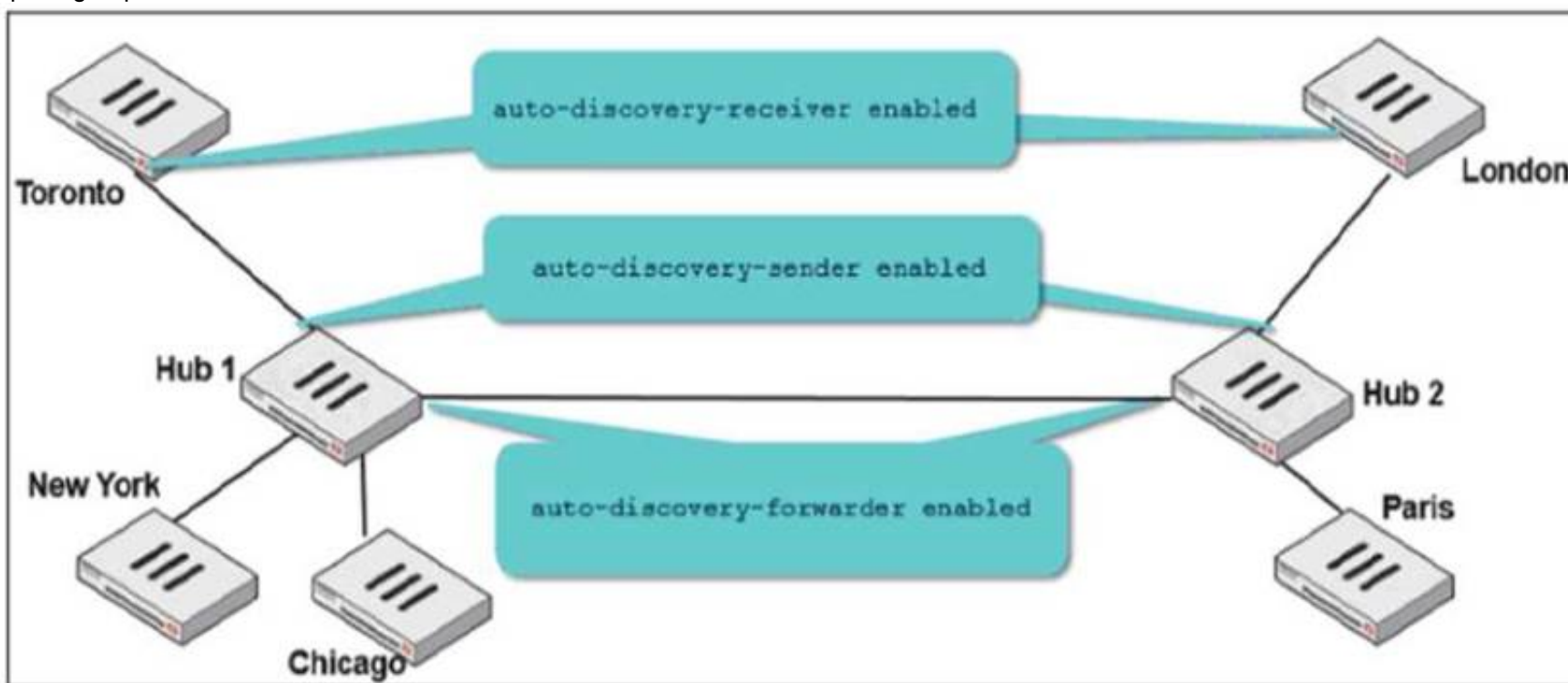
An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A. After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The 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 5

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 6

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 7

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
rpd_b_link_id=800000000 rpd_b_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 8

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 9

What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

- A. The ISDB is dynamically updated and reduces administrative overhead.
- B. The ISDB requires application control to maintain signatures and perform load balancing.
- C. The ISDB applies rules to traffic from specific sources, based on application type.
- D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Answer: AD

NEW QUESTION 10

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

- A. The objects are saved in the ADOM common object database.
- B. It does not support meta fields.
- C. It uses templates to configure SD-WAN on managed devices.
- D. It supports normalized interfaces for SD-WAN member configuration.

Answer: AC

Explanation:

Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.<https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-new-features/794804/new-sd-wan-template>

NEW QUESTION 10

Refer to the exhibits.

```
dcl_fgt # show vpn ipsec phase1-interface T_INET_1_0
config vpn ipsec phase1-interface
  edit "T_INET_1_0"
    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 psksecret ENC
GayzHJ/UhxCc9FYtwas5o4rkNCMjjjNUEj4Q4f2NS6I65RIVF9zum6sJALsU9Cg+1jsXz3ZtIM+WNkHLsXkHqydgS
G/2x8Vp9Rcht6zKHPEctOcFVbaG+Ue03Rw41pmGP/Z3rIz3tdXJxfYSzKjRqggqahsmDovkrKRHTVFU1zA072t6W
iPL9co/Zf3cX+Qpnmm38MQ==
    next
end
```

```
dcl_fgt # diagnose vpn tunnel list name T_INET_1_0_0
list ipsec tunnel by names in vd 0

-----
name=T_INET_1_0_0 ver=2 serial=7 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 dst_mtu=0
dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=tunnel/255 mode=dial_inst/3 encap=none/8832
options[2280]=rgwy-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0
parent=T_INET_1_0 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=17 olast=23464 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=T_INET_1_0_0 proto=0 sa=1 ref=2 serial=1 add-route
  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=20683 type=00 soft=0 mtu=1280 expire=972/0B replaywin=2048
      seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1790/1800
  dec: spi=02f9844e esp=aes key=16 7fb5011247248d3a45ac3d802d8c8d64
      ah=sha1 key=20 bb217ce87ae060f27823b005005233811993a303
  enc: spi=ffc6576a esp=aes key=16 825bddbc5c995feb70411a773867c2d0
      ah=sha1 key=20 02db4176f7f21fae7d141526099a707f639893f1
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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 table.
- B. The phase 1 configuration supports the network-overlay setting.
- C. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
- D. Dead peer detection is disabled.

Answer: AB

NEW QUESTION 11

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 13

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 16

Refer to the exhibit.


```
config vpn ipsec phase1-interface
edit "FIRST_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "first-group"
    set psksecret fortinet1
next
edit "SECOND_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "second-group"
    set psksecret fortinet2
next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

- A. Specify a unique peer ID for each dial-up VPN interface.
- B. Use different proposals are used between the interfaces.
- C. Configure the IKE mode to be aggressive mode.
- D. Use unique Diffie Hellman groups on each VPN interface.

Answer: AC

NEW QUESTION 20

Refer to the exhibits.
Exhibit A

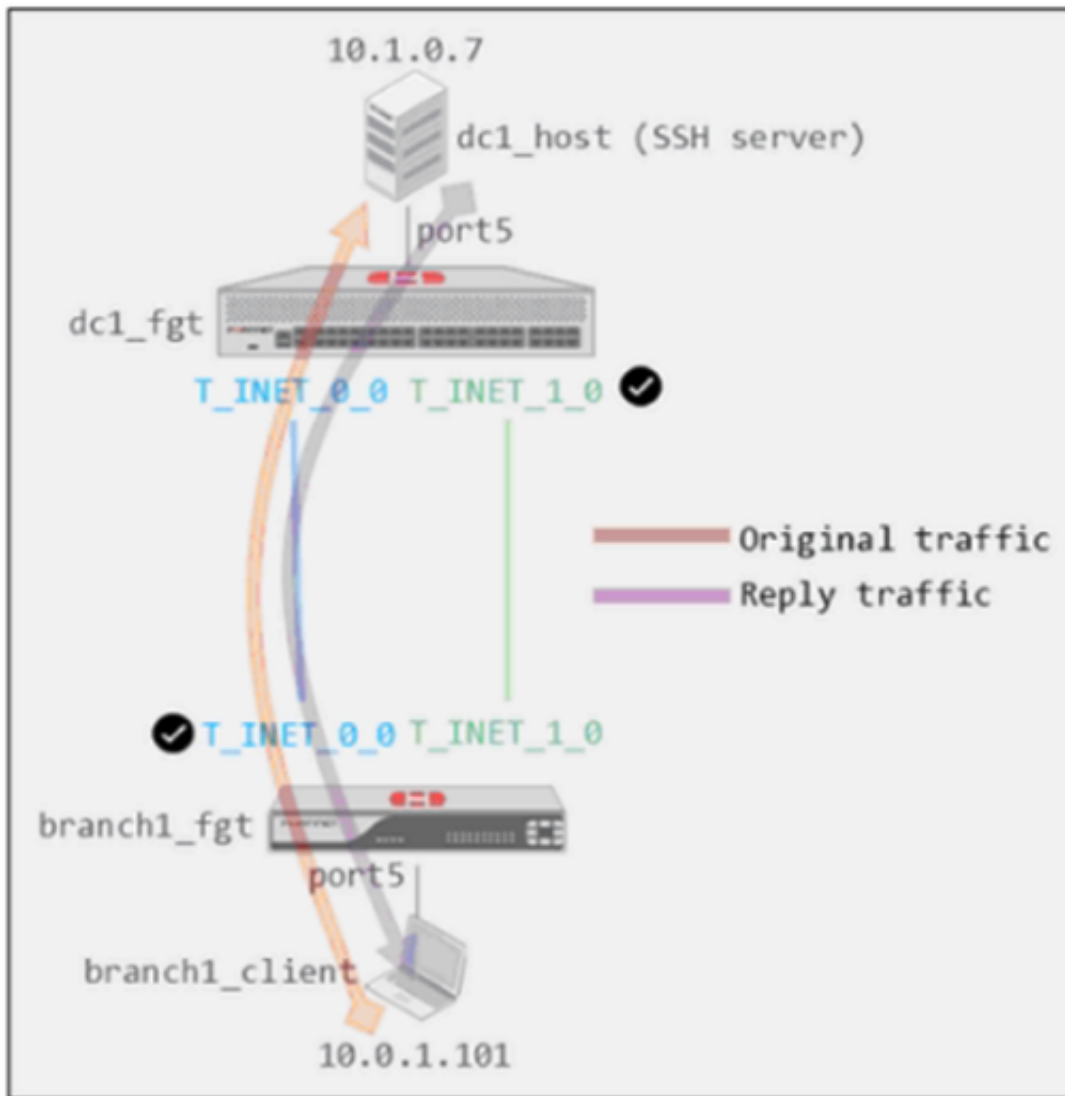


Exhibit B

```
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 25

Refer to the exhibit.

Edit Performance SLA

Name

VPN_HTTP

IP Version

IPv4

IPv6

Probe Mode

Active

Passive

Prefer Passive

Protocol

Ping

TCP ECHO

UDP ECHO

HTTP

TWAMP

DNS

TCP

Server

10.1.0.7

Port

0

Participants

All SD-WAN Members

Specify

T_INET_0_0

T_INET_1_0

T_MPLS_0

3 Entries Selected

Enable Probe Packets

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 27

Which two interfaces are considered overlay links? (Choose two.)

- A. LAG
- B. IPsec
- C. Physical
- D. GRE

Answer: BD

NEW QUESTION 29

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.0 Practice Test Here](#)