

## Exam Questions NSE7\_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

[https://www.2passeasy.com/dumps/NSE7\\_SDW-7.0/](https://www.2passeasy.com/dumps/NSE7_SDW-7.0/)



### NEW QUESTION 1

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 2

Refer to the exhibit.

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

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

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

**Answer: CD**

### NEW QUESTION 3

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

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

**Answer: AD**

### NEW QUESTION 4

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 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 are three key routing principles in SD-WAN? (Choose three.)

- A. FortiGate performs route lookups for new sessions only.
- B. Regular policy routes have precedence over SD-WAN rules.
- C. SD-WAN rules have precedence over ISDB routes.
- D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
- E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

**Answer:** BDE

#### NEW QUESTION 9

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two )

- A. Traffic has matched none of the FortiGate policy routes.
- B. Matched traffic failed RPF and was caught by the rule.
- C. The FIB lookup resolved interface was the SD-WAN interface.
- D. An absolute SD-WAN rule was defined and matched traffic.

**Answer:** AC

#### NEW QUESTION 10

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), health-check(VPN_PING)
Members(3):
  1: Seq_num(3 T_INET_0_0), alive, packet loss: 2.000%, selected
  2: Seq_num(4 T_MPLS_0), alive, packet loss: 4.000%, selected
  3: Seq_num(5 T_INET_1_0), alive, packet loss: 12.000%, 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 link-cost-factor packet-loss
  set link-cost-threshold 0
  set priority-members 5 3 4
next
end
```

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured packet loss will make T\_INET\_1\_0 the new preferred member?

- A. When all three members have the same packet loss.
- B. When T\_INET\_0\_0 has 4% packet loss.
- C. When T\_INET\_0\_0 has 12% packet loss.
- D. When T\_INET\_1\_0 has 4% packet loss.

**Answer:** A

#### NEW QUESTION 10

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

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

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 14

Which components make up the secure SD-WAN solution?

- A. Application, antivirus, and URL, and SSL inspection
- B. Datacenter, branch offices, and public cloud
- C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
- D. Telephone, ISDN, and telecom network.

**Answer:** C

#### NEW QUESTION 16

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
[-] logger	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 17

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 22

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 24

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 25

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 29**

Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

- A. get router info routing-table all
- B. diagnose debug application ike
- C. diagnose vpn tunnel list
- D. get ipsec tunnel list

**Answer:** B

**Explanation:**

IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations.

- diagnose debug console timestamp enable
- diagnose vpn ike log filter clear
- diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
- diagnose debug application ike -1
- diagnose debug enable

**NEW QUESTION 31**

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

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

**Answer:** A

**NEW QUESTION 33**

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 36**

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 37

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 38

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 43

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 45

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 48

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/UhxCc9FYtwas5o4rkNCMjjNUEj4Q4f2NS6I65RIVF9zum6sJALsU9Cg+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 53

Refer to the exhibits.

Exhibit A

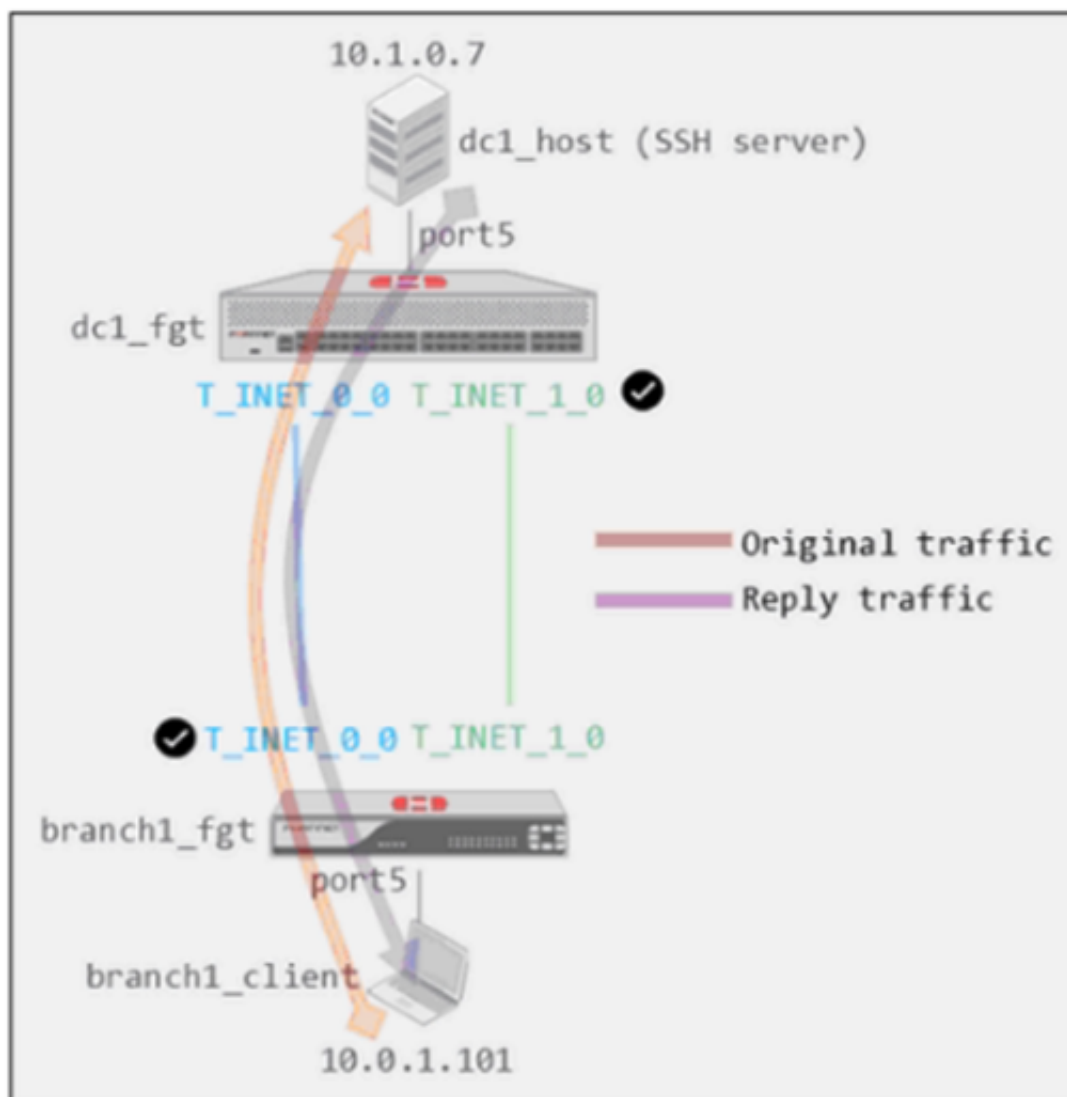


Exhibit B

```
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 57

Refer to the exhibits.

Exhibit A

### Edit Traffic Shaping Policy

IP Version: **IPv4** IPv6

Name: Limit\_Youtube

Status: **Enable** Disable

Comments:   
0/255

**If Traffic Matches:**

Source Internet Service: ☐

Source Address: LAN-net

Source User: +

Source User Group: +

Destination Internet Service: ☐

Destination Address: all

Schedule: +

Service: ALL

Application: YouTube

Application Category: +

Application Group: +

URL Category: +

Type Of Service: 0x00

Type Of Service Mask: 0x00

**Then:**

Action: **Apply Shaper** Assign Group

Outgoing Interface: underlay

Shared Shaper: low-priority

Reverse Shaper: low-priority

Per-IP Shaper: +

Differentiated Services: ☐

Differentiated Services Reverse: ☐

Exhibit B

### Edit Firewall Policy

ID: 1

Name: DIA

ZTNA: **Disable** Full ZTNA IP/MAC filtering

Incoming Interface: LAN

Outgoing Interface: underlay

Source Internet Service: ☐

IPv4 Source Address: LAN-net

IPv6 Source Address: +

Source User: +

Source User Group: +

FSSO Groups: +

Destination Internet Service: ☐

IPv4 Destination Address: all

IPv6 Destination Address: +

Service: ALL

Schedule: always

Action: Deny **Accept** IPSEC

Inspection Mode: **Flow-based** Proxy-based

**Firewall/Network Options**

NAT: ☒ NAT NAT46 NAT64

IP Pool Configuration: **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port: ☐

Protocol Options: default

**Disclaimer Options**

Display Disclaimer: ☐

**Security Profiles**

SSL/SSH Inspection: deep-inspection

Decrypted Traffic Mirror: +

**Traffic Shaping Options**

Shared Shaper: +

Reverse Shaper: +

Per-IP Shaper: +

**Logging Options**

Log Allowed Traffic: No Log Log Security Events **Log All Sessions**

☐ Capture Packets

☐ Generate Logs when Session Starts

Exhibit A shows the traffic shaping policy and exhibit B shows the firewall policy.

The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic.

Based on the policies shown in the exhibits, what configuration change must be made so FortiGate performs traffic shaping on YouTube traffic?

- A. Destination internet service must be enabled on the traffic shaping policy.
- B. Application control must be enabled on the firewall policy.
- C. Web filtering must be enabled on the firewall policy.
- D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

**Answer:** B

#### NEW QUESTION 62

.....



## 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/](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