

# Fortinet

## Exam Questions NSE7\_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2



### NEW QUESTION 1

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**

### NEW QUESTION 2

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: BD**

### NEW QUESTION 3

Refer to the exhibit.

```
# get router info routing-table all
...
B      10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
        [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
        [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

The device exchanges routes using IBGP.

Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

- A. Each BGP route is three hops away from the destination.
- B. ibgp-multipath is disabled.
- C. additional-path is enabled.
- D. You can run the get router info routing-table database command to display the additional paths.

**Answer: CD**

### NEW QUESTION 4

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 5**

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
edit "T_INET_0_0"
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
set comments "[created by FMG VPN Manager]"
set idle-timeout enable
set idle-timeoutinterval 5
set auto-discovery-receiver enable
set remote-gw 100.64.1.1
set psksecret ENC
6D5rVsaKlMeAyVYt1z95BS24Psew76lwY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfACzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpxNkHxpH
LReOFShoH0lSPFKz5IYCVA==
next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD- WAN?

- A. You must set ike-version to 1.
- B. You must enable net-device.
- C. You must enable auto-discovery-sender.
- D. You must disable idle-timeout.

**Answer: B**

**NEW QUESTION 6**

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
23.212.249.108	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2

  

Security	General	Source	Destination
APP Count	Log ID	Country	Country
Level	Session ID	Device ID	End User ID
	Session ID	Device Name	Endpoint ID
	Session ID	IP	Host Name
	Session ID	Interface	IP
	Session ID	Interface Role	Interface
	Session ID	NAT IP	
	Session ID	NAT Port	
	Session ID	Port	
	Session ID	Source	
	Session ID	UEBA Endpoint ID	
	Session ID	UEBA User ID	

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:** BC

**Explanation:**

Study guide 7.2 Page 191

**NEW QUESTION 7**

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:** D

**NEW QUESTION 8**

Exhibit.

```
# diagnose sys sdwan health-check status

Health Check(Level3 DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The exhibit shows the output of the command diagnose sys sdwan health-check status

collected on a FortiGate device. Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

- A. The health-check VPN\_PING orders the members according to the lowest jitter.  
 B. The interface T\_INET\_1 missed one SLA target.  
 C. There is no SLA criteria configured for the health-check Level3\_DNS.  
 D. The interface T\_INET\_0 missed three SLA targets.

**Answer:** AC

**Explanation:**

According to the FortiGate / FortiOS 6.4.2 Administration Guide, the health check status command displays the status of the health check probes for each SD-WAN member interface. The output includes the following information:

- ? state: the current state of the interface, either alive or dead
- ? packet-loss: the percentage of packets lost during the health check
- ? latency: the average round-trip time in milliseconds
- ? jitter: the variation in latency
- ? mos: the mean opinion score, a measure of voice quality
- ? bandwidth: the available bandwidth in kilobits per second for each direction (up, down, bi)
- ? sla map: a bitmap that indicates which SLA criteria are met or failed

Based on the exhibit, the following statements are correct:

- ? The health-check VPN\_PING orders the members according to the lowest jitter. This means that the interface with the lowest jitter value is listed first, followed by the next lowest, and so on. In the exhibit, the order is T\_MPLS, T\_INET\_1, and T\_INET\_0.
- ? There is no SLA criteria configured for the health-check Level3\_DNS. This means that the health check does not use any SLA parameters to determine the state of the interface. In the exhibit, the sla map value is 0x0 for both port1 and port2, indicating that no SLA criteria are applied.

**NEW QUESTION 9**



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 10

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Service disabled caused by no destination.
Members(2):
  1: Seq_num(4 T_INET_1_0), alive, selected
  2: Seq_num(5 T_MPLS_0), alive, selected
Src address(1):
  10.0.1.0-10.0.1.255

branch1_fgt # get router info bgp community 65000:10
VRF 0 BGP table version is 3, local router ID is 10.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight RouteTag Path
*>i10.1.0.0/24      10.202.1.254             0    100     0         1 i <-/1>
* i                 10.203.1.254             0    100     0         1 i <-/->

Total number of prefixes 1
```

## Exhibit B

```
branch1_tgt (1) # show
config service
  edit 1
    set name "Corp"
    set route-tag 10
    set src "LAN-net"
    set priority-zone "overlay"
  next
end

config router bgp
...
  config neighbor
    edit "10.202.1.254"
      set soft-reconfiguration enable
      set interface "T_INET_1_0"
      set remote-as 65000
      set route-map-in "dcl-lan-rm"
      set update-source "T_INET_1_0"
    next
    edit "10.203.1.254"
      set soft-reconfiguration enable
      set interface "T_MPLS_0"
      set remote-as 65000
      set route-map-in "dcl-lan-rm"
      set update-source "T_MPLS_0"
    next
  end
...
config router route-map
  edit "dcl-lan-rm"
    config rule
      edit 1
        set match-community "dcl-lan-cl"
        set set-route-tag 1
      next
    end
  next
end
```

Exhibit A shows the SD-WAN rule status and the learned BGP routes with community 65000:10. Exhibit B shows the SD-WAN rule configuration, the BGP neighbor configuration, and the route map configuration. The administrator wants to steer corporate traffic using routes tags in the SD-WAN rule ID 1. However, the administrator observes that the corporate traffic does not match the SD-WAN rule ID 1. Based on the exhibits, which configuration change is required to fix issue?

- A. In the dcl-lab-rm route map configuration, set set-route-tag to 10.
- B. In SD-WAN rule ID 1, change the destination to use ISDB entries.
- C. In the BGP neighbor configuration, apply the route map dcl-lab-rm in the outbound direction.
- D. In the dcl-lab-rm route map configuration, unset match-community.

**Answer: C**

### NEW QUESTION 10

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 11

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 15

Which statement about SD-WAN zones is true?

- A. An SD-WAN zone can contain only one type of interface.
- B. An SD-WAN zone can contain between 0 and 512 members.
- C. You cannot use an SD-WAN zone in static route definitions.
- D. You can configure up to 32 SD-WAN zones per VDOM.

**Answer: D**

**Explanation:**

SD-WAN zones are a group of interfaces that share the same SD-WAN settings, such as health check, SLA, and load balancing. Some characteristics of SD-WAN zones are:

? An SD-WAN zone can contain different types of interfaces, such as physical, VLAN, aggregate, and tunnel interfaces1.

? An SD-WAN zone can contain up to 512 members1.

? You can use an SD-WAN zone in static route definitions, as long as the destination interface is also an SD-WAN zone1.

? You can configure up to 32 SD-WAN zones per VDOM1.

**NEW QUESTION 16**

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

**Answer: A**

**NEW QUESTION 17**

Refer to the exhibit.

Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
edit "T_INET_1"
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 auto-discovery-sender enable
set paksecret ENC MXtFGKOxLV+x4p3e9Xq2HGJcU+QOgg5YMqiXb2T73f2pSXS/
jv9oshWeQ1NEjOJEtUqqD8mAw7G2ZLTlsR3/ihAaAY4tvjveS+9CuTn00J2tuddoM9
uz4vaBTNbNrh3/EhbJytsCag==
next
end
```

Exhibit B

```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
-----
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=:10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag_rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=42955943 ad=/0
stat: rxp=32 txp=0 rxh=1280 txh=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/08 replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=shal key=20 f0d3ac8192d2e79fbbe29162f9ccf406flal61b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6alf9fe5ab38b953dd4782f
ah=shal key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_lgwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=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. Most Voted
- C. The phase 1 configuration supports the network-overlay setting.
- D. Most Voted
- E. FortiGate facilitated the negotiation of the T\_INET\_1\_0\_0 ADVPN shortcut over T\_INET\_1\_0.
- F. Dead peer detection is disabled.

**Answer: AC**

**NEW QUESTION 20**

Refer to the exhibits.

**Exhibit A**

**Exhibit B**

Exhibit A shows two IPsec templates to define Branch\_IPsec\_1 and Branch\_IPsec\_2. Each template defines a VPN tunnel. Exhibit B shows the error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device. Which statement best explain the cause for this issue?

- A. You can assign only one template with a tunnel of type static to each FortiGate device
- B. You can define only one IPsec tunnel from branch devices to HUB1.
- C. You can assign only one IPsec template to each FortiGate device.
- D. You should review the branch1\_fgt configuration for the already configured tunnel with the name HUB1-VPN2.

**Answer: C**

**Explanation:**

The error message in Exhibit B indicates a conflicting template assignment. This occurs because FortiManager does not allow the assignment of multiple IPsec templates that define VPN tunnels with the same name or settings to the same FortiGate device. The conflict arises from trying to assign a second IPsec template to a device that already has one assigned. References: This is based on Fortinet's best practices and administrative guidelines which state that each FortiGate device should be assigned a unique IPsec template to avoid configuration conflicts.

**NEW QUESTION 22**

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 24**

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
rpdn_link_id=80000000 rpdn_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 25

What three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

- A. You can apply a system template and a CLI template to the same FortiGate device.
- B. A CLI template can be of type CLI script or Perl script.
- C. A template group can include a system template and an SD-WAN template.
- D. A template group can contain CLI templates of both types.
- E. Templates are applied in order, from top to bottom.

**Answer:** BDE

### Explanation:

According to the FortiManager Administration Guide, provisioning templates are used to configure FortiGate devices in a consistent and efficient way. There are different types of templates, such as system, IPsec, SD-WAN, certificate, and CLI templates. Some characteristics of provisioning templates are:

- ? You can apply a system template and a CLI template to the same FortiGate device, as long as they do not have conflicting settings<sup>1</sup>.
- ? A CLI template can be of type CLI script or Perl script. A CLI script template contains FortiOS CLI commands, while a Perl script template contains Perl code that can generate FortiOS CLI commands<sup>2</sup>.
- ? A template group can include a system template and an SD-WAN template, as well as other types of templates. A template group is a collection of templates that can be applied to multiple devices at once<sup>3</sup>.
- ? A template group can contain CLI templates of both types, as long as they do not have conflicting settings<sup>2</sup>.
- ? Templates are applied in order, from top to bottom. The order of the templates in a template group determines the order in which they are applied to the devices<sup>3</sup>.

### NEW QUESTION 29

Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

- A. When configuring an SD-WAN rule, you can select multiple SLA targets of the same performance SLA.
- B. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements.
- C. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy.
- D. Member metrics are measured only if an SLA target is configured.

**Answer:** BD

### NEW QUESTION 33

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

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

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

Answer: BC

NEW QUESTION 37

What are two common use cases for remote internet access (RIA)? (Choose two.)

- A. Provide direct internet access on spokes
- B. Provide internet access through the hub
- C. Centralize security inspection on the hub
- D. Provide thorough inspection on spokes

Answer: BC

Explanation:

\* B. Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.

\* C. Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NEW QUESTION 42

Refer to the exhibits. Exhibit A -

Edit Traffic Shaping Policy

IP Version

IPv4IPv6

Name

Limit\_YouTube

Status

EnableDisable

Comments

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 ShaperAssign Group

Outgoing Interface

underlay

Shared Shaper

low-priority

Reverse Shaper

low-priority

Per-IP Shaper

Differentiated Services

Differentiated Services Reverse

Exhibit B -

The screenshot displays the FortiGate configuration interface for a Firewall Policy. The left pane shows the 'Edit Firewall Policy' configuration, and the right pane shows the 'Traffic Shaping Options'.

**Firewall Policy Configuration (Left Pane):**

- ID:** 1
- Name:** DIA
- ZTNA:** Disabled
- Incoming Interface:** LAN
- Outgoing Interface:** underlay
- Source Internet Service:** LAN-net
- IPv4 Source Address:** LAN-net
- IPv6 Source Address:** +
- Source User:** +
- Source User Group:** +
- FSSO Groups:** +
- Destination Internet Service:** all
- 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

**Traffic Shaping Options (Right Pane):**

- 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: C**

#### NEW QUESTION 46

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

- A. It ensures consistent settings between phase1 and phase2.
- B. It guides the administrator to use Fortinet recommended settings.
- C. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- D. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

**Answer: AB**

#### Explanation:

The use of an IPsec recommended template offers the advantage of ensuring consistent settings between phase1 and phase2 (A), which is essential for the stability and security of the IPsec tunnel. Additionally, it guides the administrator to use Fortinet's recommended settings (B), which are designed to optimize performance and security based on Fortinet's best practices. References: The benefits of using IPsec recommended templates are outlined in Fortinet's SD-WAN documentation, which emphasizes the importance of consistency and adherence to recommended configurations.

#### NEW QUESTION 51

Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

- A. Encapsulating Security Payload (ESP)
- B. Secure Shell (SSH)
- C. Internet Key Exchange (IKE)
- D. Security Association (SA)

**Answer: AC**

#### NEW QUESTION 53

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 56

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 [I], 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 58

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
2v9n4Urfk0W4jj8vWI+KywxBG4ZDT7jWHKd8YaL8j4+pRpY0x/N7mSgc7VL0BW2ZHQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+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**

#### NEW QUESTION 60

Refer to the exhibit.

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

Based on the exhibit, which action does FortiGate take?

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

**Answer: A**

#### NEW QUESTION 64

The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks. What are three mandatory post-run tasks that must be performed? (Choose three.)

- A. Create policy packages for branch devices.
- B. Assign an sdwan\_id metadata variable to each device (branch and hub).
- C. Configure routing through overlay tunnels created by the SD-WAN overlay template.
- D. Assign a branch\_id metadata variable to each branch device.
- E. Configure SD-WAN rules.

**Answer: ABC**

#### NEW QUESTION 68

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. Three packets are exchanged between an initiator and a responder instead of six packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.



**Answer:** AC

#### NEW QUESTION 71

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 75

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in a hub-and-spoke topology? (Choose two.)

- A. VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.
- B. FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- C. IPsec recommended template guides the administrator to use Fortinet recommended settings.
- D. IPsec recommended template ensures consistent settings between phase1 and phase2

**Answer:** BC

#### Explanation:

According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:

? FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.

? IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

#### NEW QUESTION 80

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 84

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 85

What are two benefits of choosing packet duplication over FEC for data loss correction on noisy links? (Choose two.)

- A. Packet duplication can leverage multiple IPsec overlays for sending additional data.
- B. Packet duplication does not require a route to the destination.
- C. Packet duplication supports hardware offloading.
- D. Packet duplication uses smaller parity packets which results in less bandwidth consumption.

**Answer:** AC

#### NEW QUESTION 86

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 88

Which statement about using BGP routes in SD-WAN is true?

- A. Learned routes can be used as dynamic destinations in SD-WAN rules.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure AS path prepending.
- D. You must use external BGP.

**Answer:** A

#### NEW QUESTION 89

.....

## 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-7.2 Practice Exam Features:

- \* NSE7\_SDW-7.2 Questions and Answers Updated Frequently
- \* NSE7\_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE7\_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_SDW-7.2 Practice Test Here](#)**