



**Fortinet**

## **Exam Questions NSE7\_SDW-7.2**

Fortinet NSE 7 - SD-WAN 7.2

### NEW QUESTION 1

Which diagnostic command can you use to show the SD-WAN rules, interface information, and state?

- A. diagnose sys sdwan service
- B. diagnose sys sdwan route-tag-list
- C. diagnose sys sdwan member
- D. diagnose sys sdwan neighbor

**Answer: A**

### NEW QUESTION 2

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 3

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 4

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
6D5rVsaKlMeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+Wuszpmlv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH0ISPFKz5IYCVA==
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 5

Which two statements about the SD-WAN zone configuration are true? (Choose two.)

- A. The service-sla-tie-break setting enables you to configure preferred member selection based on the best route to the destination.
- B. You can delete the default zones.
- C. The default zones are virtual-wan-link and SASE.
- D. An SD-WAN member can belong to two or more zones.

Answer: AC

## NEW QUESTION 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
23.212.249.144	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	APP Count	1
General	Log ID	0000000013
	Session ID	799
	Session Display	not
	Virtual Domain	not
Source	Country	Reserved
	Device ID	FGW401TH42000077
	Device Name	branch1_fgt
	IP	10.0.1.101
	Interface	port1
	Interface Role	undefined
	NAT IP	192.2.0.9
	NAT Port	55042
	Port	55042
	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	23.212.249.144
	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: BC

## Explanation:

Study guide 7.2 Page 191

## NEW QUESTION 7

Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)

- A. FortiGate does not consider the source address of the packet when matching an SD- WAN rule for local-out traffic.
- B. By default, local-out traffic does not use SD-WAN.
- C. By default, FortiGate does not check if the selected member has a valid route to the destination.
- D. You must configure each local-out feature individually, to use SD-WAN.

Answer: BD

## NEW QUESTION 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(99999999), bandwidth-dw(99999999), bandwidth-bi(199999998) 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 on1. 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 interface2. 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 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
origin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=0.0.0.0/0.0.0.0
hook=pre 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
rpdh_link_id=ff000002 rpdh_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

**Explanation:**

The `snat-route-change` option is enabled by default. This option enables FortiGate to re- evaluate the routing table and select a new egress interface if the next hop IP address changes. This option only applies to sessions in the dirty state. Sessions in the log state are not affected by routing changes.

**NEW QUESTION 10**

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 exhibit.

```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.10
hook-post dir-org act=snat 10.0.1.10:2246->8.8.8.8(192.168.73.132:62662)
hook-pre dir-reply act=dnat 8.8.8.8:62662->192.168.73.132:0(10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_lnk_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

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

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

Answer: C

NEW QUESTION 12

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_fgt (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 16

Refer to the exhibit.

```
config system sdwan
  set status enable
  set load-balance source-dest-ip-based
  config zone
    edit "virtual-wan-link"
    next
    edit "SASE"
    next
    edit "underlay"
    next
  end
  config members
    edit 1
      set interface "port1"
      set zone "underlay"
      set gateway 192.2.0.2
    next
    edit 2
      set interface "port2"
      set zone "underlay"
      set gateway 192.2.0.10
    next
  end
  ...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD- WAN rules?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. All traffic from a source IP is sent to the same interface.
- C. All traffic from a source IP is sent to the most used interface.
- D. All traffic from a source IP to a destination IP is sent to the least used interface.

**Answer:** A

**Explanation:**

Study Guide 7.2, page 176.

#### NEW QUESTION 20

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 21

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 22

Refer to the exhibit.



```
config system settings
  set firewall-session-dirty check-new
end
```

Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

- A. FortiGate flushes all sessions.
- B. FortiGate terminates the old sessions.
- C. FortiGate does not change existing sessions.
- D. FortiGate evaluates new sessions.

**Answer:** CD

**Explanation:**

FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new. The results is that FortiGate evaluates only new session against the new firewall policy.

**NEW QUESTION 23**

Refer to the exhibits.

Exhibit A

```
config duplication
  edit 1
    set srcaddr "10.0.1.0/24"
    set dstaddr "10.1.0.0/24"
    set srcintf "port5"
    set dstintf "overlay"
    set service "ALL"
    set packet-duplication force
  next
end

branch1_fgt # diagnose sys sdwan zone
Zone SASE index=2
  members(0):
Zone overlay index=4
  members(3): 19(T_INET_0_0) 20(T_INET_1_0) 21(T_MPLS_0)
Zone underlay index=3
  members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
  members(0):

1.274665 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275788 T_INET_0_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275790 T_INET_1_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275801 T_MPLS_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.278365 T_INET_1_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.278553 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.875308 T_INET_1_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on FortiGate acting as the sender. Exhibit B shows the sniffer output on a FortiGate acting as the receiver.

The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T\_INET\_1\_0.

Based on the output shown in the exhibits, which two reasons can cause the observed behavior? (Choose two.)

- A. On the receiver FortiGate, packet-de-duplication is enabled.
- B. The ICMP echo request packets sent over T\_INET\_0\_0 and T\_MPLS\_0 were dropped along the way.
- C. The ICMP echo request packets received over T\_INET\_0\_0 and T\_MPLS\_0 were offloaded to NPU.
- D. On the sender FortiGate, duplication-max-num is set to 3.

**Answer:** AD

**NEW QUESTION 27**

Exhibit A –



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

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

Exhibit B –

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

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

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

Answer: B

NEW QUESTION 32

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

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

Answer: AD

NEW QUESTION 34

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 settings1.
- ? 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 commands2.
- ? 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 once3.
- ? A template group can contain CLI templates of both types, as long as they do not have conflicting settings2.
- ? 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 devices3.

NEW QUESTION 39

Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

- A. http
- B. icmp
- C. twamp
- D. dns

**Answer:** AD

**Explanation:**

Performance SLA (Service Level Agreement) protocols are used in SD-WAN to monitor the quality and performance of various network services. The two protocols that specifically allow for verifying a specific value in the server response are:

? HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It allows for fetching resources, such as HTML documents. You can configure an HTTP performance SLA to send specific requests (e.g., GET or POST) and then check if the response body contains a particular string or value. This is useful for validating web server functionality and content delivery.

? DNS (Domain Name System): DNS is responsible for translating domain names into IP addresses. A DNS performance SLA can be set up to query a specific domain and verify that the returned IP address or other DNS record values match what is expected. This helps ensure proper name resolution and accessibility of resources.

**NEW QUESTION 41**

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 46**

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 50**

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 54**

Refer to the exhibits. Exhibit A -

Edit Traffic Shaping Policy

IP Version

IPv4IPv6

Name

Limit\_YouTube

Status

EnableDisable

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 ShaperAssign 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

DisableFull ZTNAIP/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

DenyAcceptIPSEC

Inspection Mode

Flow-basedProxy-based

Firewall/Network Options

NAT

NATNAT46NAT64

IP Pool Configuration

Use Outgoing Interface AddressUse 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 LogLog Security EventsLog 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 57

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 60**

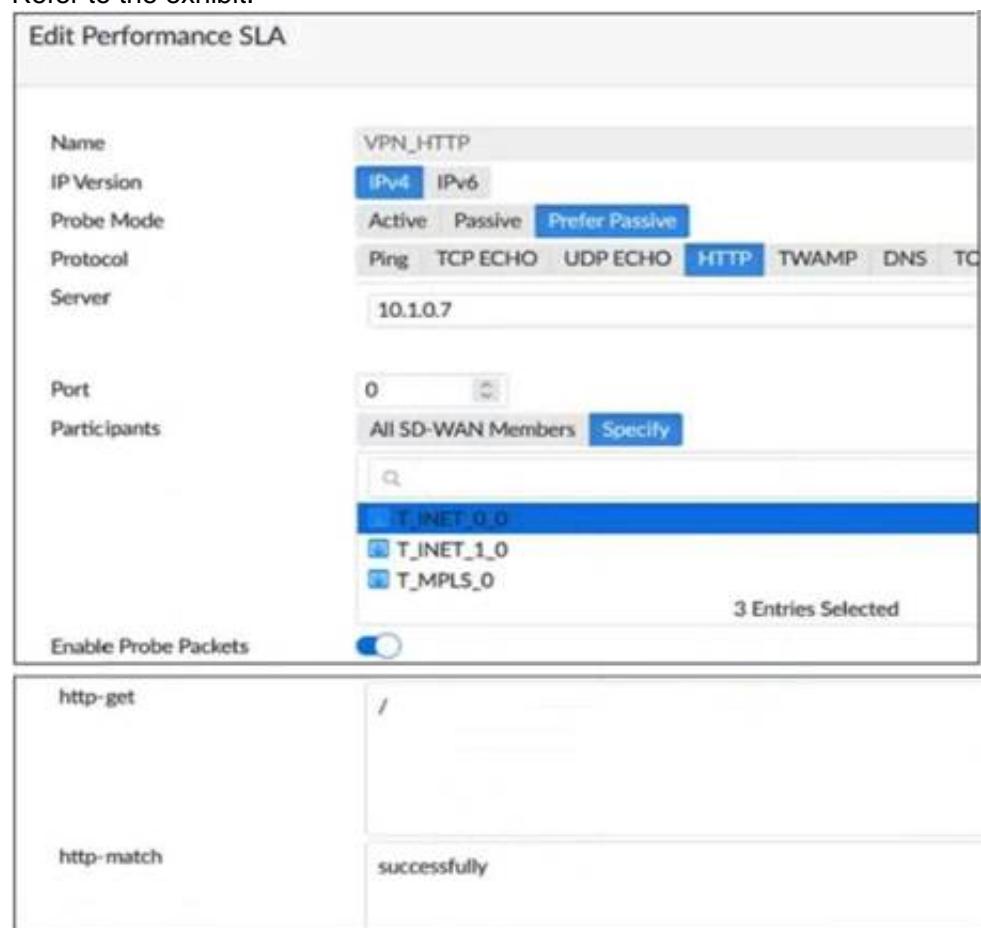
In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 61**

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 TC
Server	10.1.0.7
Port	0
Participants	All SD-WAN Members Specify
	<input type="text"/> <ul style="list-style-type: none"> <li>T_INET_0_0</li> <li>T_INET_1_0</li> <li>T_MPLS_0</li> </ul> 3 Entries Selected
Enable Probe Packets	<input checked="" type="checkbox"/>
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 63**

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-fmg>

**NEW QUESTION 68**

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 73

Which two statements describe how IPsec phase 1 main mode id 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 77

Refer to the exhibits. Exhibit A -

Edit Performance SLA

Name

Level3\_DNS

IP Version

IPv4

IPv6

Probe Mode

Active

Passive

Prefer Passive

Protocol

Ping

TCP ECHO

UDP ECHO

HTTP

TW

Server

4.2.2.1

4.2.2.2

Participants

All SD-WAN Members

Specify

port1

port2

2 Entries

Enable Probe Packets

SLA Targets

+ Add Target

Link Status

Interval

500

Milliseconds

Failure Before Inactive

3

(max 3600)

Restore Link After

2

(max 3600)

Action When Inactive

Update Static Route

Cascade Interfaces

Exhibit B -

```
branch1_fgt # diagnose sys sdwan member | grep port
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

branch1_fgt # get router info routing-table all | grep port
S* 0.0.0.0/0 [1/0] via 192.2.0.2, port1
   [1/0] via 192.2.0.10, port2
S 8.8.8.8/32 [10/0] via 192.2.0.11, port2
C 10.0.1.0/24 is directly connected, port5
S 172.16.0.0/16 [10/0] via 172.16.0.2, port4
C 172.16.0.0/29 is directly connected, port4
C 192.2.0.0/29 is directly connected, port1
C 192.2.0.8/29 is directly connected, port2
C 192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status. If port2 is detected dead by FortiGate, what is the expected behavior?

- A. Port2 becomes alive after three successful probes are detected.
- B. FortiGate removes all static routes for port2.
- C. The administrator manually restores the static routes for port2, if port2 becomes alive.
- D. Host 8.8.8.8 is reachable through port1 and port2.

**Answer: B**

**Explanation:**

This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

**NEW QUESTION 82**

Refer to the exhibit.

```
config router bgp
  set as 65000
  set router-id 10.1.0.1
  set ibgp-multipath enable
  set additional-path enable
  set additional-path-select 3
  config neighbor-group
    edit "Branches_INET_0"
      set interface "T_INET_0_0"
      set remote-as 65000
      set update-source "T_INET_0_0"
    next
    edit "Branches_INET_1"
      set interface "T_INET_1_0"
      set remote-as 65000
      set update-source "T_INET_1_0"
    next
    edit "Branches_MPLS"
      set interface "T_MPLS_0"
      set remote-as 65000
      set update-source "T_MPLS_0"
    next
  end
  config neighbor-range
    edit 1
      set prefix 10.201.1.0 255.255.255.0
      set neighbor-group "Branches_INET_0"
    next
    edit 2
      set prefix 10.202.1.0 255.255.255.0
      set neighbor-group "Branches_INET_1"
    next
    edit 3
      set prefix 10.203.1.0 255.255.255.0
      set neighbor-group "Branches_MPLS"
    next
  end
end
...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.

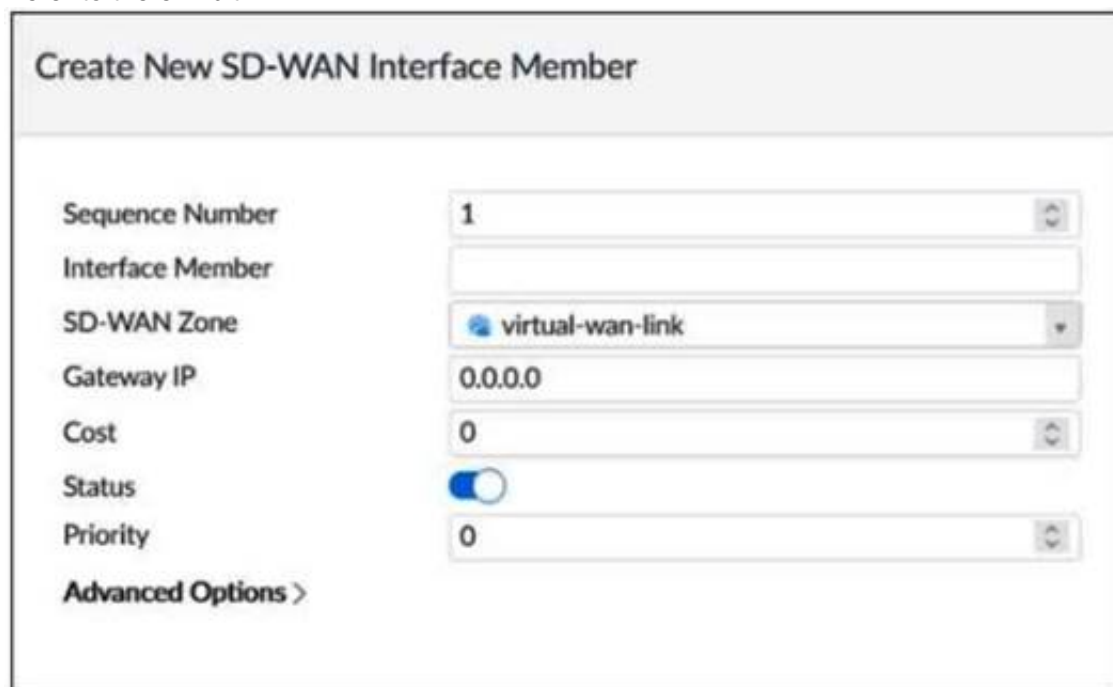
Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

- A. Set additional-path to send
- B. Enable route-reflector-client
- C. Set advertisement-interval to the number of additional paths to advertise
- D. Set adv-additional-path to the number of additional paths to advertise
- E. Enable soft-reconfiguration

**Answer:** ABD

#### NEW QUESTION 84

Refer to the exhibit.



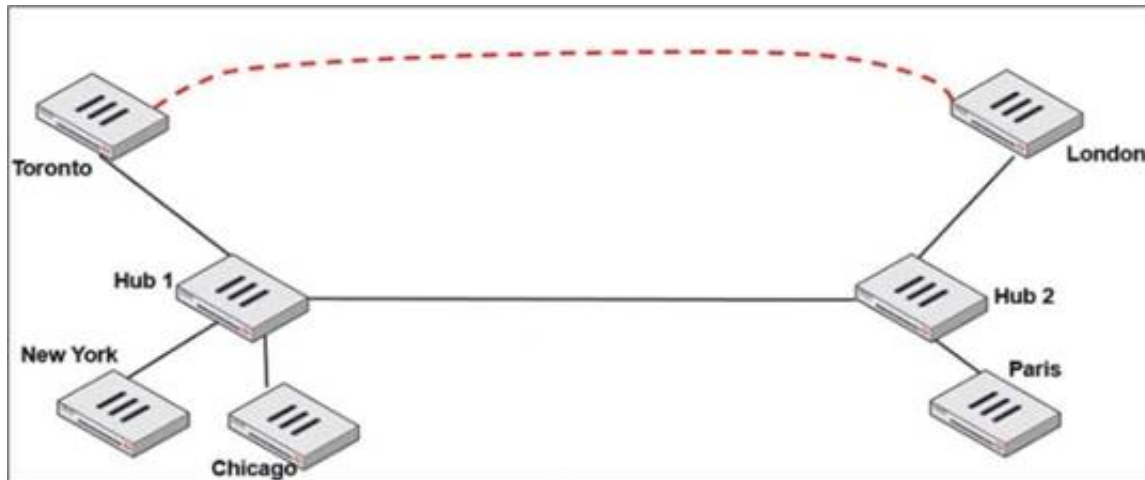
Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)

- A. Cost
- B. Interface member
- C. Priority
- D. Gateway IP

**Answer:** BD

#### NEW QUESTION 86

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2.

Which two configuration settings are required for Toronto and London spokes to establish an ADVPN shortcut? (Choose two.)

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

**Answer:** AB

#### NEW QUESTION 91

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 95

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 97

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 102

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 107

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

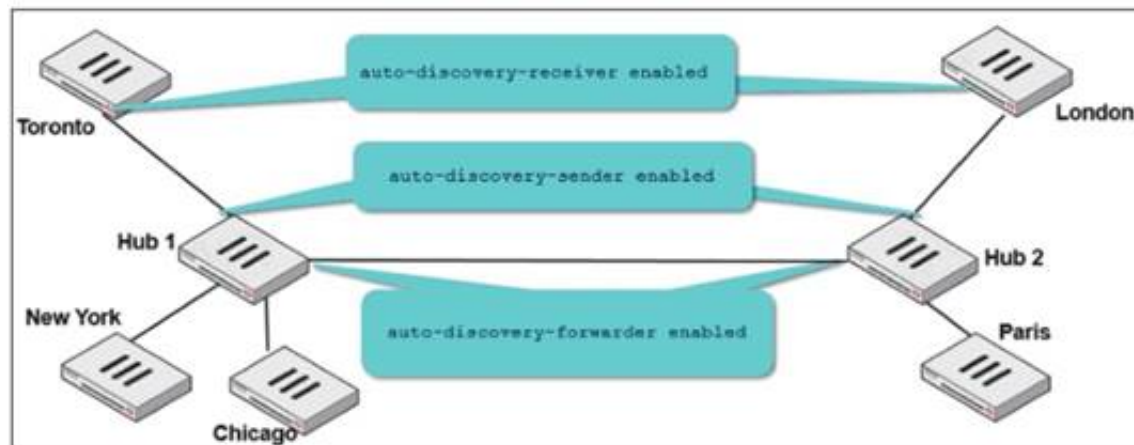
- A. Learned routes can be used as dynamic destinations in SD-WAN rules.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure AS path prepending.
- D. You must use external BGP.

**Answer:** A

#### NEW QUESTION 108

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 112

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 113

Which two statements reflect the benefits of implementing the ADVPN solution to replace conventional VPN topologies? (Choose two.)

- A. It creates redundant tunnels between hub-and-spokes, in case failure takes place on the primary links.
- B. It dynamically assigns cost and weight between the hub and the spokes, based on the physical distance.
- C. It ensures that spoke-to-spoke traffic no longer needs to flow through the tunnels through the hub.
- D. It provides direct connectivity between all sites by creating on-demand tunnels between spokes.

**Answer: CD**

#### NEW QUESTION 118

.....

## 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](#)**