

# Fortinet

## Exam Questions NSE7\_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2



### NEW QUESTION 1

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 2

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

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

**Answer: AE**

### NEW QUESTION 3

Which action fortigate performs on the traffic that is subject to a per-IP traffic shaper of 10 Mbps?

- A. FortiGate applies traffic shaping to the original traffic direction only.
- B. FortiGate shares 10 Mbps of bandwidth equally among all source IP addresses.
- C. RIAS
- D. Fortigate limits each source ip address to a maximum bandwidth of 10 Mbps.
- E. FortiGate guarantees a minimum of 10 Mbps of bandwidth to each source IP address.

**Answer: C**

### 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

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

**Answer: BC**

**NEW QUESTION 6**

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 7**

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	sec-1		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		port1
23.212.249.144	HTTPS	GoToMeeting	sec-2		port2
23.205.106.86	HTTPS	GoToMeeting	sec-2		port2

Security	Value
APP Count	1
Level	info
General	
App ID	000000013
Session ID	789
User Display	www
Virtual Domain	nat
Source	
Country	Belgium
Device ID	FDV4017M42000077
Device Name	branch1_fgt
IP	10.0.1.101
Interface	port3
Interface Role	unclassified
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	151
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: BC**

**Explanation:**

Study guide 7.2 Page 191

**NEW QUESTION 8**

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 9**

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 10**

Refer to the exhibits.

Exhibit A

The screenshot shows the configuration for a service named 'Critical-DIA'. Key details include:
 

- Service:** Critical-DIA
- Identity:** Device ID is FGVM01TM22000077, Device Name is branch1\_fgt.
- Type:** Sub Type is sdwan, Type is event.
- Alerts:** Level is notice.
- General:** Log Description is SDWAN status, Log ID is 0113022923, Message is 'Service prioritized by performance metric will be redirected in sequence order.', Sequence Number is 2,1, Virtual Domain is root.
- Others:** Date/Time is 23:57:29, Destination End User ID is 3, Destination Endpoint ID is 3, Device Time is 2022-03-04 14:57:27, Event Time is 1646434647595788893, Event Type is Service, Metric is latency, Service ID is 1, Time Stamp is 2022-03-04 23:57:29, Time Zone is -0800, UEBA Endpoint ID is 3, UEBA User ID is 3, logver is 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=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd link_id= 80000000 rpd_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 14**

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 16**

Refer to the Exhibits:

**Exhibit A**   **Exhibit B**

**Link Status**

Check interval:  ms

Failures before inactive:

Restore link after:  check(s)

**Actions when Inactive**

Update static route:

**Exhibit A**   **Exhibit B**

```

NGFW-1 # diagnose sys sdwan health-check
Health Check (Ping):
Seq (1 port1): state (alive), packet-loss (0.000%) latency
(6.196), jitter (0.079) sla_map=0x0
Seq (2 port2): state (dead), packet-loss (6.000%) sla_map=0x0
    
```

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members. Based on the exhibits, which statement is correct?

- A. The dead member interface stays unavailable until an administrator manually brings the interface back.
- B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
- C. Static routes using port2 are active in the routing table.
- D. FortiGate has not received three consecutive requests from the SLA server configured for port2.

**Answer: C**

**NEW QUESTION 17**

Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

- A. update-source
- B. set-route-tag
- C. holdtime-timer
- D. link-down-failover

**Answer: CD**

**NEW QUESTION 19**

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 22**

Refer to the exhibits.

**Exhibit A**

IPsec Template Branch\_IPsec\_1

Name	Type	Outgoing Interface
HUB1-VPN1	Static	\$(ISP1)

IPsec Template Branch\_IPsec\_2

Name	Type	Outgoing Interface
HUB1-VPN2	Static	\$(ISP2)

**Exhibit B**

invalid template assignment - conflicting template assignment scope: device branch1\_fgt, vdom root, x  
 \_ipsec template [Branch\_IPsec\_1] and [Branch\_IPsec\_2]

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 24**

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 29**

Exhibit A –

#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
<b>Physical (10)</b>						
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
<b>Aggregate (1)</b>						
11	fortlink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
<b>Tunnel (3)</b>						
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	
<b>EMAC VLAN (1)</b>						
15	vt_lan_ts	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
<b>SD-WAN Zone (2)</b>						
16	virtual-wan-link	SD-WAN Zone				
17	SASE	SD-WAN Zone	SASE			

#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
<b>Static Route (2)</b>								
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
<b>Implicit (2-2 / Total: 1)</b>							
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 31**

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 34**

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 36**

Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

- A. diagnose sys sdwan zone
- B. diagnose sys sdwan service
- C. diagnose sys sdwan member
- D. diagnose sys sdwan interface

**Answer:** C

**NEW QUESTION 39**

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 40**

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 41**

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: C**

**NEW QUESTION 44**

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 48**

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 51**

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 54**

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 55**

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 58**

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

```

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 59**

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 62**

Refer to the exhibit.

### Create New SD-WAN Interface Member

Sequence Number	<input type="text" value="1"/>
Interface Member	<input type="text"/>
SD-WAN Zone	<input type="text" value="virtual-wan-link"/>
Gateway IP	<input type="text" value="0.0.0.0"/>
Cost	<input type="text" value="0"/>
Status	<input checked="" type="checkbox"/>
Priority	<input type="text" value="0"/>
<b>Advanced Options &gt;</b>	

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 64**

Which type statements about the SD-WAN members are true? (Choose two.)

- A. You can manually define the SD-WAN members sequence number.
- B. Interfaces of type virtual wire pair can be used as SD-WAN members.
- C. Interfaces of type VLAN can be used as SD-WAN members.
- D. An SD-WAN member can belong to two or more SD-WAN zones.

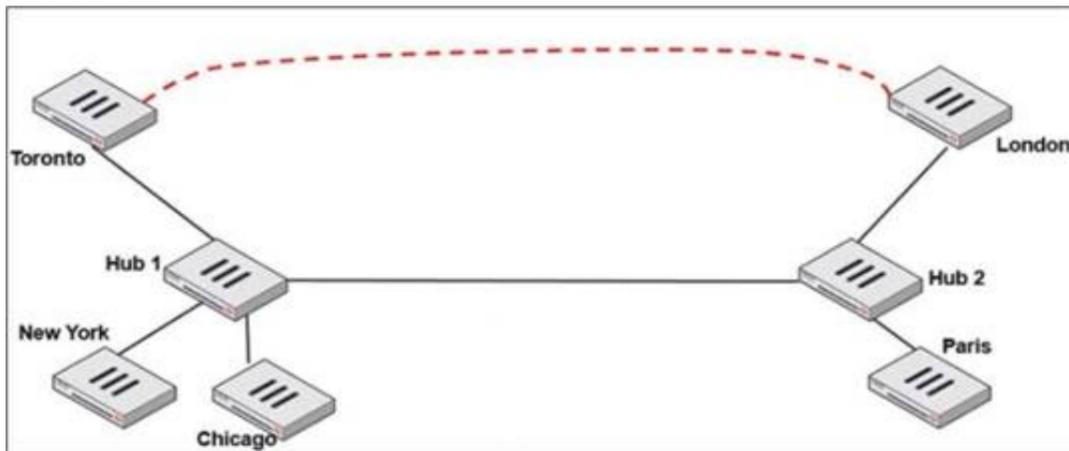
**Answer:** AC

**Explanation:**

SD-WAN members can be manually ordered by changing their sequence number (A), which allows administrators to prioritize the interfaces according to the routing requirements. Also, VLAN interfaces can be used as SD-WAN members (C), providing flexibility in network design and the use of existing VLAN infrastructure within the SD-WAN setup.

**NEW QUESTION 65**

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 68**

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 71**

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

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

**Answer: BD**

**NEW QUESTION 74**

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 75**

.....

## 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 First Try
- \* NSE7\_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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