

# 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.Portals(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**

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
LReOFShoH01SPFKz5IYCVA==
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 3**

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 4**

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(1 port1), alive, selected
  2: Seq_num(2 port2), alive, selected
Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
Src address(1):
  10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(1):
  1: Seq_num(2 port2), alive, selected
Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
Src address(1):
  10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
         [1/0] via 192.2.0.10, port2
...
```

Exhibit B

Destination IP	Service	Application	Security Event Unit	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	APP Count	0
Level	Level	notice
General	Log ID	0000000013
	Session ID	769
	Tran Display	nat
	Virtual Domain	nat
Source	Country	Reserved
	Device ID	FDVH017H42000077
	Device Name	branch1_fgt
	IP	10.0.1.103
	Interface	port3
	Interface Role	undrflowd
	NAT IP	192.2.0.9
	NAT Port	55043
	Port	55042
	Source	10.0.1.103
	UEBA Endpoint ID	1025
	UEBA User ID	3
Destination	Country	United States
	End User ID	3
	Endpoint ID	155
	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 5**

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 6**

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), heath-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 7

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 8

Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

- A. Interface-based shaping mode
- B. Reverse-policy shaping mode
- C. Shared-policy shaping mode
- D. Per-IP shaping mode

**Answer: A**

## Explanation:

Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

## NEW QUESTION 9

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 10

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 MXtFGK0xLV+x4p3e9Xq2HGJoU+QOgg5YMq1Xb2T73fZpSKS/
jv9oshWeQ1NEjOJEtqqQD8mAw7G22LT1sR3/ihAaAY4tvjveS+9CuTn00J2tuddoM9
uz4vaBTNbNrh3/KhbJytsCag==
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: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/0B 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 8547efb42d148c6692fb2af0d0d01ff12d
ah=shal key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6a1f9fe5ab38b953dd4782f
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 10

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 13

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 17**

Exhibit A –

+ Create New ▾ Edit Delete Where Used Collapse All Column Settings ▾ More ▾							
<input type="checkbox"/>	#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
<input type="checkbox"/>	▼ Physical (10)						
<input type="checkbox"/>	1	port1	Physical	port1	Manual	203.0.113.1/255.255.255.2	PING
<input type="checkbox"/>	2	port2	Physical	port2	Manual	203.0.113.9/255.255.255.2	PING
<input type="checkbox"/>	3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	4	port4	Physical	port4	Manual	172.16.0.9/255.255.255.24	PING
<input type="checkbox"/>	5	port5	Physical	port5	Manual	10.0.2.254/255.255.255.0	PING
<input type="checkbox"/>	6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	10	port10	Physical	port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT
<input type="checkbox"/>	▼ Aggregate (1)						
<input type="checkbox"/>	11	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
<input type="checkbox"/>	▼ Tunnel (3)						
<input type="checkbox"/>	12	nat.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	13	i2t.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	14	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	▼ EMAC VLAN (1)						
<input type="checkbox"/>	15	vl_lan_1s	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
<input type="checkbox"/>	▼ SD-WAN Zone (2)						
<input type="checkbox"/>	16	virtual-wan-link	SD-WAN Zone				
<input type="checkbox"/>	17	SASE	SD-WAN Zone	SASE			

+ Create New ▾ Edit Delete Column Settings ▾									
<input type="checkbox"/>	#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
<input type="checkbox"/>	▼ Static Route (2)								
<input type="checkbox"/>	1	1	0.0.0.0/0.0.0.0	203.0.113.2	port1	10	0	Enable	
<input type="checkbox"/>	2	2	0.0.0.0/0.0.0.0	203.0.113.10	port2	10	0	Enable	

Exhibit B –

+ Create New ▾ Edit Delete Section ▾ Policy Lookup Collapse All Column Settings ▾ View Mode ▾								
<input type="checkbox"/>	#	Name	From	To	Source	Destination	Schedule	Service
<input type="checkbox"/>	1	Internet_Access	port5	port1	all	all	always	ALL
<input type="checkbox"/>	▼ Implicit (2-2 / Total: 1)							
<input type="checkbox"/>	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 18**

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 22**

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 26

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 29

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 34

Refer to the exhibit.

```
config system virtual-wan-link
  set status enable
  set load-balance-mode source-ip-based
  config members
    edit 1
      set interface "port1"
      set gateway 100.64.1.254
      set source 100.64.1.1
      set cost 15
    next
    edit 2
      set interface "port2"
      set gateway 100.64.2.254
      set priority 10
    next
  end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

- A. Set priority 10.
- B. Set cost 15.
- C. Set load-balance-mode source-ip-ip-based.
- D. Set source 100.64.1.1.

**Answer:** AB

#### NEW QUESTION 36

Which components make up the secure SD-WAN solution?

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



D. Telephone, ISDN, and telecom network.

**Answer: C**

### NEW QUESTION 38

Refer to the exhibits.

Exhibit A

```
config system sdwan
  config health-check
    edit "Passive"
      set detect-mode passive
      set members 3 4
    next
  end
end

config system sdwan
  config service
    edit 1
      set name "Facebook-YouTube"
      set src "all"
      set internet-service enable
      set internet-service-app-ctrl 15832 31077
      set health-check "Passive"
      set priority-member 3 4
      set passive-measurement enable
    next
  end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B

```
config firewall policy
  edit 1
    set name "DIA"
    set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
    set srcintf "port5"
    set dstintf "underlay"
    set action accept
    set srcaddr "LAN-net"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set passive-wan-health-measurement enable
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set application-list "default"
    set logtraffic all
    set auto-asic-offload disable
    set nat enable
  next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
  members(2): 3(port1) 4(port2)
```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

- A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
- B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
- C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
- D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

**Answer: AD**

### Explanation:

Study Guide 7.2, pages 103 - 104. Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

### NEW QUESTION 39

Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.] seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg="Find an existing
session, id=000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg="exceeded shaper limit, drop"
```

Which conclusion about the packet debug flow output is correct?

- A. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
- B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
- C. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
- D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

**Answer:** D

#### NEW QUESTION 42

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

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

**Answer:** AC

#### NEW QUESTION 47

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 51

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 56

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 58**  
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 62**  
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.

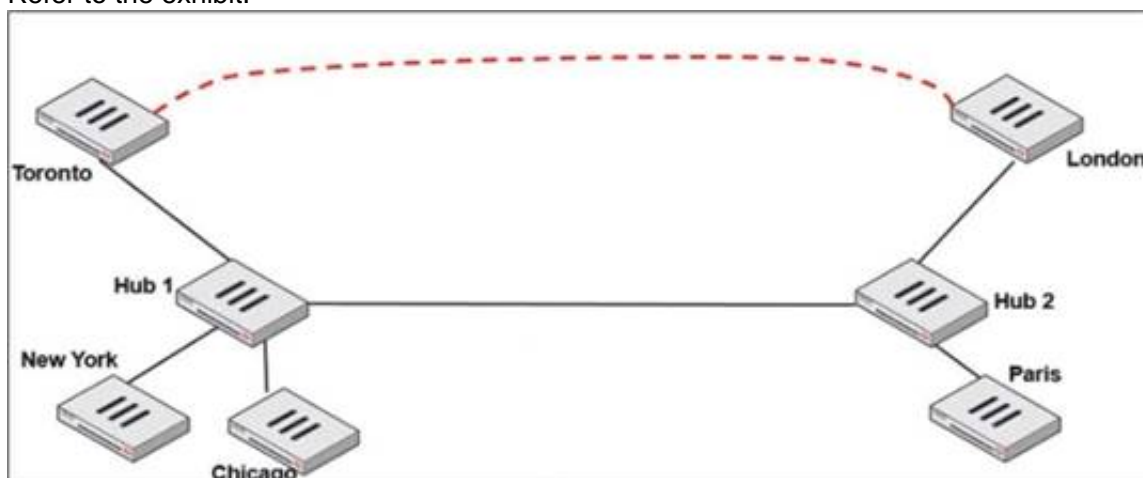
Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

- 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 67

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 72

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 73

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 74

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 78

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 83

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 84

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 86**

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**

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 91**

.....

## 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](#)**