

## NSE7\_SDW-7.2 Dumps

### Fortinet NSE 7 - SD-WAN 7.2

[https://www.certleader.com/NSE7\\_SDW-7.2-dumps.html](https://www.certleader.com/NSE7_SDW-7.2-dumps.html)



**NEW QUESTION 1**

Refer to the exhibit.

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

The device exchanges routes using IBGP.

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

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

**Answer:** CD

**NEW QUESTION 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**

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
    6DSrVsaKlMeAyVYt1z95BS24Psew76lwY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+Wuszpmlv8rRzrVh
    7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
    LRe0FSHoH0lSPFKz5IYCVA==
    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 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**

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		port2
23.205.106.86	HTTPS	GoToMeeting	sec:2		port2

Security	APP Count	1
Level	Level	1
General	Log ID	0000000013
	Session ID	789
	Trans Display	enat
	Virtual Domain	nat
Source	Country	Reserved
	Device ID	FDVH017H42000077
	Device Name	branch1_fgt
	IP	10.0.1.103
	Interface	port1
	Interface Role	undrflow
	NAT IP	192.2.0.9
	NAT Port	55042
	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 7

Which two statements about SD-WAN central management are true? (Choose two.)

- A. It does not allow you to monitor the status of SD-WAN members.
- B. It is enabled or disabled on a per-ADOM basis.
- C. It is enabled by default.
- D. It uses templates to configure SD-WAN on managed devices.

**Answer: BD**

#### NEW QUESTION 8

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 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-post dir=org act=snat 10.0.1.101:34676->128.66.0.1:22(192.2.0.1:34676)
hook-pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:34676(10.0.1.101:34676)
hook-post dir=reply act=noop 128.66.0.1:22->10.0.1.101:34676(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
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 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
origin->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
rpdh_link_id= 80000000 rpdh_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 10**

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service 1

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

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

   Network          Next Hop           Metric LocPrf Weight RouteTag Path
*>i10.1.0.0/24      10.202.1.254             0    100      0         1 i <-/->
* 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 15

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 19**

What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

- A. FEC supports hardware offloading.
- B. FEC improves reliability of noisy links.
- C. FEC transmits parity packets that can be used to reconstruct packet loss.
- D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

**Answer:** BC

**NEW QUESTION 22**

Refer to the Exhibits:

Exhibit A

Exhibit B

Link Status

Check interval500ms

Failures before inactive3

Restore link after2check(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 27**

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 29**

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+x4p3e9Kq2HGJcU+QOgg5YMqiXb2T73fZpSX5/
jv9oshWeQ1NEjOJEtUqqD8mAw7G22LTisR3/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 encaps=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=1774/08 replaywin=2048
seqno=1 ean=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=shal key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6alf9fe3ab38b953dd4782f
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 32

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 result is that FortiGate evaluates only new session against the new firewall policy.

#### NEW QUESTION 37

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 40

Refer to the exhibit.

```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=39 expire=3593 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
state=may_dirty npu
orgin->sink: org pre->post, reply pre->post dev=7->5/5->7 gw=10.10.10.1/10.9.31.160
hook=pre dir=org act=noop 10.9.31.160:7932->10.0.1.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.0.1.7:22->10.9.31.160:7932(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00045e02 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan mbr seq=1 sdwan_service_id=1
rpidb_link_id=80000000 rpidb_svc_id=0 ngfwid=n/a
npu_state=0x4000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/76, ipid=76/64,
vlan=0x0000/0x0000
vlifid=76/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/2
reflect info 0:
dev=7->6/6->7
npu_state=0x4000800
npu info: flag=0x00/0x81, offload=0/8, ips_offload=0/0, epid=0/76, ipid=0/65, vlan=0x0000/0x0000
vlifid=0/65, vtag_in=0x0000/0x0000 in_npu=0/1, out_npu=0/1, fwd_en=0/0, qid=0/2
total reflect session num: 1
total session 1

# diagnose netlink interface list

if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate appliance that supports hardware offloading. Based on the information shown in the exhibits, which two statements about the session are true? (Choose two.)

- A. The reply direction of the asymmetric traffic flows from port2 to port3.
- B. The auxiliary session can be offloaded to hardware.
- C. The original direction of the symmetric traffic flows from port3 to port2.
- D. The main session cannot be offloaded to hardware.

**Answer: AB**

#### NEW QUESTION 41

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 46

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 51

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 56

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 57

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 59

Exhibit.

```
7: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9 resport=500 locport=500 outintf="port2" cookies="773c72b40060051d/529ac435532959b6" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.1 vpntunnel="T_INET_1" tunnelip=N/A tunnelid=2595348112 tunneltype="ipsec" duration=3581 sentbyte=386431 rcvbyte=387326 nextstat=600 advpnsc=0
```

```
8: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.0.9 locip=172.16.0.1 resport=500 locport=500 outintf="port4" cookies="0624890597f0096d/ed1bd5247375c46f" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_MPLS_0" tunnelip=0.0.0.0 tunnelid=2595348102 tunneltype="ipsec" duration=223 sentbyte=115040 rcvbyte=345160 nextstat=600 advpnsc=1
```

```
9: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1 resport=500 locport=500 outintf="port1" cookies="747b432459497188/6616a969a6937853" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.1 vpntunnel="T_INET_0" tunnelip=N/A tunnelid=2595348115 tunneltype="ipsec" duration=3580 sentbyte=388020 rcvbyte=387994 nextstat=600 advpnsc=0
```

The exhibit shows VPN event logs on FortiGate. In the output shown in the exhibit, which statement is true?

- A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
- B. There is one shortcut tunnel built from master tunnel T\_MPLS\_0.
- C. The VPN tunnel T\_MPLS\_0 is a shortcut tunnel.
- D. The master tunnel T\_INET\_0 cannot accept the ADVPN shortcut.

**Answer:** B

**Explanation:**

VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:

- ? logid: the log ID number
- ? type: the log type, either traffic or event
- ? subtype: the log subtype, either vpn or ipsec
- ? level: the log level, either error, warning, or notice
- ? vd: the virtual domain name
- ? logdesc: the log description
- ? msg: the log message
- ? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
- ? remip: the remote IP address
- ? locip: the local IP address
- ? remport: the remote port number
- ? locport: the local port number
- ? outintf: the outgoing interface name
- ? cookies: the IKE SA cookies
- ? user: the user name
- ? group: the user group name
- ? useralt: the alternative user name
- ? xauthuser: the XAuth user name
- ? authgroup: the XAuth user group name
- ? assignip: the assigned IP address
- ? vpntunnel: the VPN tunnel name
- ? tunnellip: the tunnel loopback IP address
- ? tunnelid: the tunnel ID number
- ? tunneltype: the tunnel type, either ipsec or ssl
- ? duration: the tunnel duration in seconds
- ? sentbyte: the number of bytes sent
- ? rcvdbyte: the number of bytes received
- ? nextstat: the next statistics interval in seconds
- ? advpnsc: the ADVPN shortcut flag, either 0 or 1 Based on the exhibit, the following statement is true:
  - ? There is one shortcut tunnel built from master tunnel T\_MPLS\_0. This means that the VPN tunnel T\_MPLS\_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T\_MPLS\_0\_0 is a shortcut tunnel that is built from the master tunnel T\_MPLS\_01. In the exhibit, the log action for T\_MPLS\_0 is tunnel-up, and the log action for T\_MPLS\_0\_0 is shortcut-up. The advpnsc flag for T\_MPLS\_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T\_MPLS\_0\_0 is 1, indicating that it is a shortcut tunnel.

**NEW QUESTION 62**

Refer to the exhibits. Exhibit A -

Edit Traffic Shaping Policy

IP Version

IPv4 IPv6

Name

Limit\_YouTube

Status

Enable Disable

Comments

If Traffic Matches:

Source Internet Service

Source Address

LAN-net

Source User

+

Source User Group

+

Destination Internet Service

Destination Address

all

Schedule

+

Service

ALL

Application

YouTube

Application Category

+

Application Group

+

URL Category

+

Type Of Service

0x00

Type Of Service Mask

0x00

Then:

Action

Apply 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 64

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 68**

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 71**

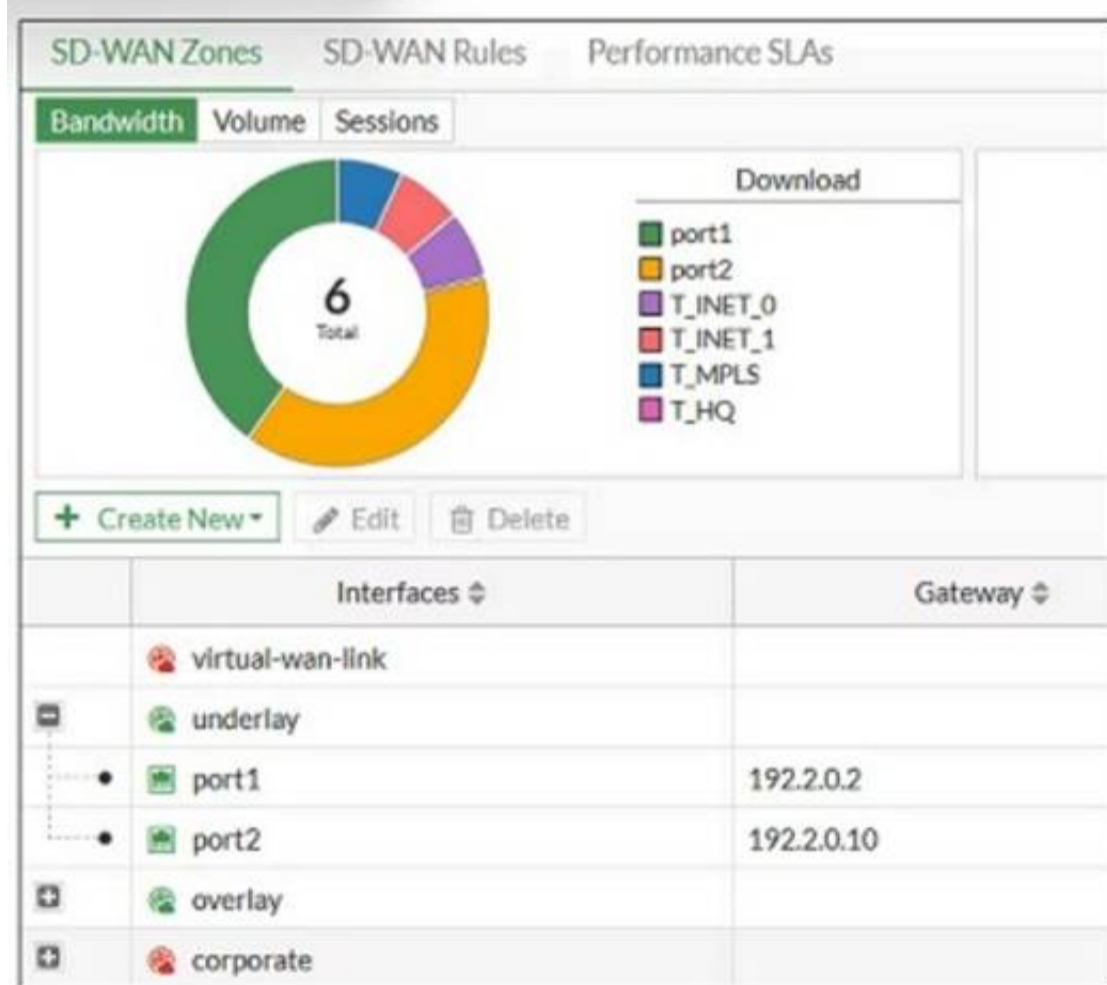
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 75**

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

- A. You can delete the virtual-wan-link zone because it contains no member.
- B. The corporate zone contains no member.
- C. You can move port1 from the underlay zone to the overlay zone.
- D. The overlay zone contains four members.

**Answer:** B

**Explanation:**

Based on the exhibit, the "corporate" zone contains no member (B). In the FortiGate GUI, zones without members do not display any interfaces listed under them, which is the case for the corporate zone in the exhibit. References: This conclusion is based on standard Fortinet GUI interpretation and the operational logic of SD-WAN zones as per Fortinet's guidelines and user interface standards.

**NEW QUESTION 76**

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 79**

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

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 81**

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 86**

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 91**

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 93**

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 94**

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 98

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

The Leader of IT Certification

visit - <https://www.certleader.com>

Exhibit A
Exhibit B

### Edit Policy

Name ⓘ
Internet Access

Incoming interface
port3

Outgoing interface
virtual-wan link

Source
all
+
x

Destination
all
+
x

Schedule
always

Service
ALL
+
x

Action
ACCEPT DENY

Inspection Mode
Flow-based Proxy-based

### Firewall / Network Options

NAT
☒

IP Pool Configuration
Use Outgoing Interface Address Use Dynamic

Preserve Source Port
☐

Protocol Options
PROT default

Exhibit A
Exhibit B

### Edit Traffic Shaping Policy

Name
inbound\_outbound\_shaper

Status
Enabled Disabled

Comments
Write a comment... 0/255

### If Traffic Matches:

Source
all
+
x

Destination
all
+
x

Schedule
☐

Service
ALL
+
x

Application ⓘ
+

URL Category
Streaming Media and Download
+
x

### Then:

Action
Apply Shaper Assign Shaping Class ID

Outgoing interface
virtual-wan link
+
x

Shared shaper
☒
guarantee-10mbps

The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy. Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

- Create a new firewall policy, and then select the SD-WAN zone as Incoming Interface.
- In the traffic shaping policy, select Assign Shaping Class ID as Action.
- In the firewall policy, select Proxy-based as Inspection Mode.
- In the traffic shaping policy, enable Reverse shaper, and then select the traffic shaper to use.

Answer: D

#### NEW QUESTION 100

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.

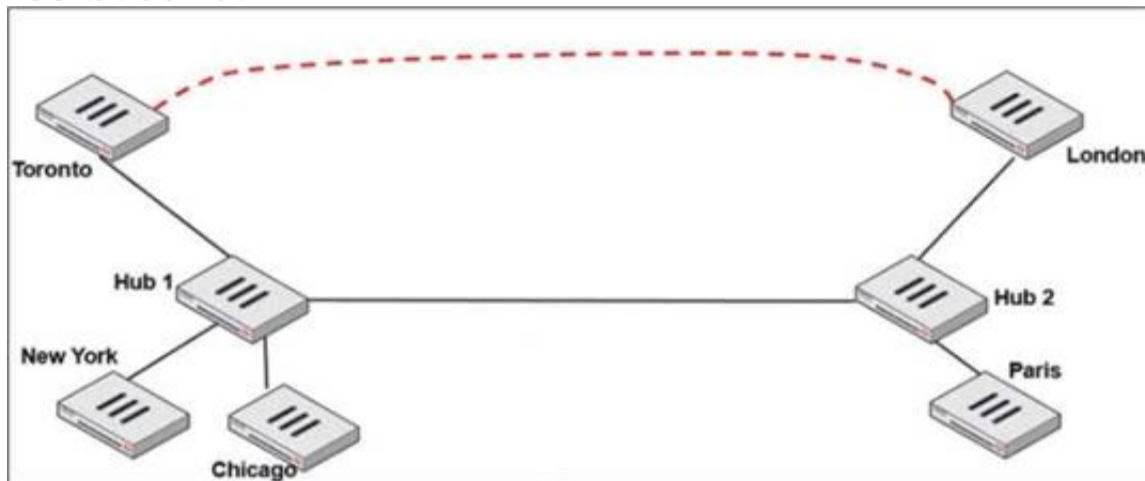
Answer: AC

#### 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 102

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 106

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 109

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 112

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
```

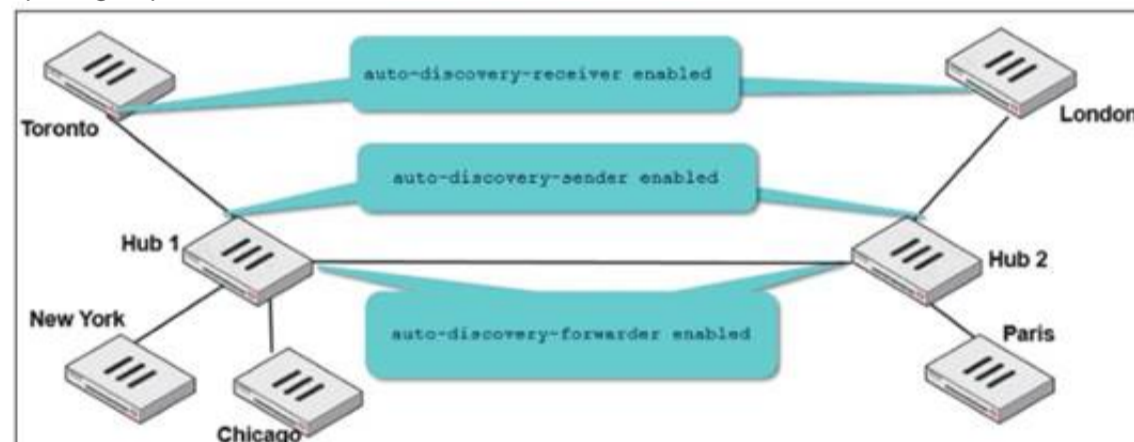
Which statement about the role of the ADVPN device in handling traffic is true?

- 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 117

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 122

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 126

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE7\_SDW-7.2 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE7\\_SDW-7.2-dumps.html](https://www.certleader.com/NSE7_SDW-7.2-dumps.html)