

# 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.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(3 T_INET_0_0), alive, selected
  2: Seq_num(4 T_INET_1_0), alive, selected
Src address(1):
  10.0.1.0-10.0.1.255

Dst address(1):
  10.0.0.0-10.255.255.255

branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4, gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4, gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S      10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1\_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T\_INET\_0\_0. However, the traffic is routed over T\_INET\_1\_0.

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

- A. The traffic matches a regular policy route configured with T\_INET\_1\_0 as the outgoing device.
- B. T\_INET\_1\_0 has a lower route priority value (higher priority) than T\_INET\_0\_0.
- C. T\_INET\_0\_0 does not have a valid route to the destination.
- D. T\_INET\_1\_0 has a higher member configuration priority than T\_INET\_0\_0.

**Answer: AC**

## NEW QUESTION 3

Refer to the exhibit.

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

The device exchanges routes using IBGP.

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

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

**Answer: CD**

**NEW QUESTION 4**

What 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 5**

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 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), 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 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 exhibits.

Exhibit A

|                         |   |
|-------------------------|---|
| Network Properties      |   |
| Service                 | Critical-DIA  |
| Identity                |   |
| Device ID               | FGVM01TM22000077  |
| Device Name             | branch1_fgt   |
| Type                    |   |
| Sub Type                | sdwan   |
| Type                    | event   |
| Alerts                  |   |
| Level                   | notice  |
| General                 |   |
| Log Description         | SDWAN status  |
| Log ID                  | 0113022923  |
| Message                 | Service prioritized by performance metric will be redirected in sequence order. |
| Sequence Number         | 2,1   |
| Virtual Domain          | root  |
| Others                  |   |
| Date/Time               | 23:57:29  |
| Destination End User ID | 3   |
| Destination Endpoint ID | 3   |
| Device Time             | 2022-03-04 14:57:27   |
| Event Time              | 1646434647595788893   |
| Event Type              | Service   |
| Metric                  | latency   |
| Service ID              | 1   |
| Time Stamp              | 2022-03-04 23:57:29   |
| Time Zone               | -0800   |
| UEBA Endpoint ID        | 3   |
| UEBA User ID            | 3   |
| logger                  | 700030237   |

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

config service
edit 1
set name "Critical-DIA"
set mode priority
set src "LAN-net"
set internet-service enable
set internet-service-app-ctrl 16354 41468 16920
set health-check "Level3_DNS"
set priority-members 1 2
next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration. Based on the exhibits, which two statements are correct? (Choose two.)

- A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
- B. Port2 has the highest member priority.
- C. Port2 has a lower latency than port1.
- D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

**Answer: AC**



NEW QUESTION 10

Refer to the exhibit.

```
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 15

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 17

Exhibit A –

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

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

Exhibit B –

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

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

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

Answer: B

NEW QUESTION 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 21

Which statement about using BGP for ADVPN is true?

- A. You must use BGP to route traffic for both overlay and underlay links.
- B. You must configure AS path prepending.
- C. You must configure BGP communities.
- D. IBGP is preferred over EBGP, because IBGP preserves next hop information.

Answer: D

Explanation:

ADVPN is a technology that allows dynamic creation of IPsec tunnels between branch sites without requiring pre-configured policies or keys. BGP is a routing protocol that can be used to exchange routes between ADVPN peers. IBGP is a type of BGP that runs between routers in the same autonomous system (AS), while EBGP is a type of BGP that runs between routers in different ASes. IBGP is preferred over EBGP for ADVPN, because IBGP preserves the next hop information of the routes, which is needed to establish the IPsec tunnels. EBGP changes the next hop information to the EBGP peer address, which may not be reachable by the ADVPN peers. Therefore, using IBGP for ADVPN avoids the need to configure additional static routes or redistribute routes between BGP and another routing protocol. References = ADVPN with BGP as the routing protocol, ADVPN, SD-WAN self-healing with BGP, Technical Tip: ADVPN with BGP as the routing protocol

The statement that IBGP is preferred over EBGP for ADVPN because IBGP preserves next hop information (D) is true. In a typical ADVPN deployment, it's beneficial to maintain next hop information across the network to ensure proper routing and optimal path selection. References: This understanding comes from my knowledge of Fortinet's SD-WAN and ADVPN configurations, where BGP's behavior in terms of next hop preservation is a key consideration.

NEW QUESTION 22

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

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

**Answer:** BD

#### NEW QUESTION 27

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 32

Which two tasks are part of using central VPN management? (Choose two.)

- A. You can configure full mesh, star, and dial-up VPN topologies.
- B. You must enable VPN zones for SD-WAN deployments.
- C. FortiManager installs VPN settings on both managed and external gateways.
- D. You configure VPN communities to define common IPsec settings shared by all VPN gateways.

**Answer:** AD

#### NEW QUESTION 36

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
report=500 locport=500 outintf="port2" cookies="773c72b4060051d/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
report=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
report=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
- ? report: 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 38

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
  factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
    2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
    3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, 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 priority-members 3 4 5
next
end
```

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured latency will make T\_MPLS\_0 the new preferred member?

- A. When T\_INET\_0\_0 and T\_MPLS\_0 have the same latency.
- B. When T\_MPLS\_0 has a latency of 100 ms.
- C. When T\_INET\_0\_0 has a latency of 250 ms.
- D. When T\_MPLS\_0 has a latency of 80 ms.

**Answer: D**

### NEW QUESTION 42

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 43

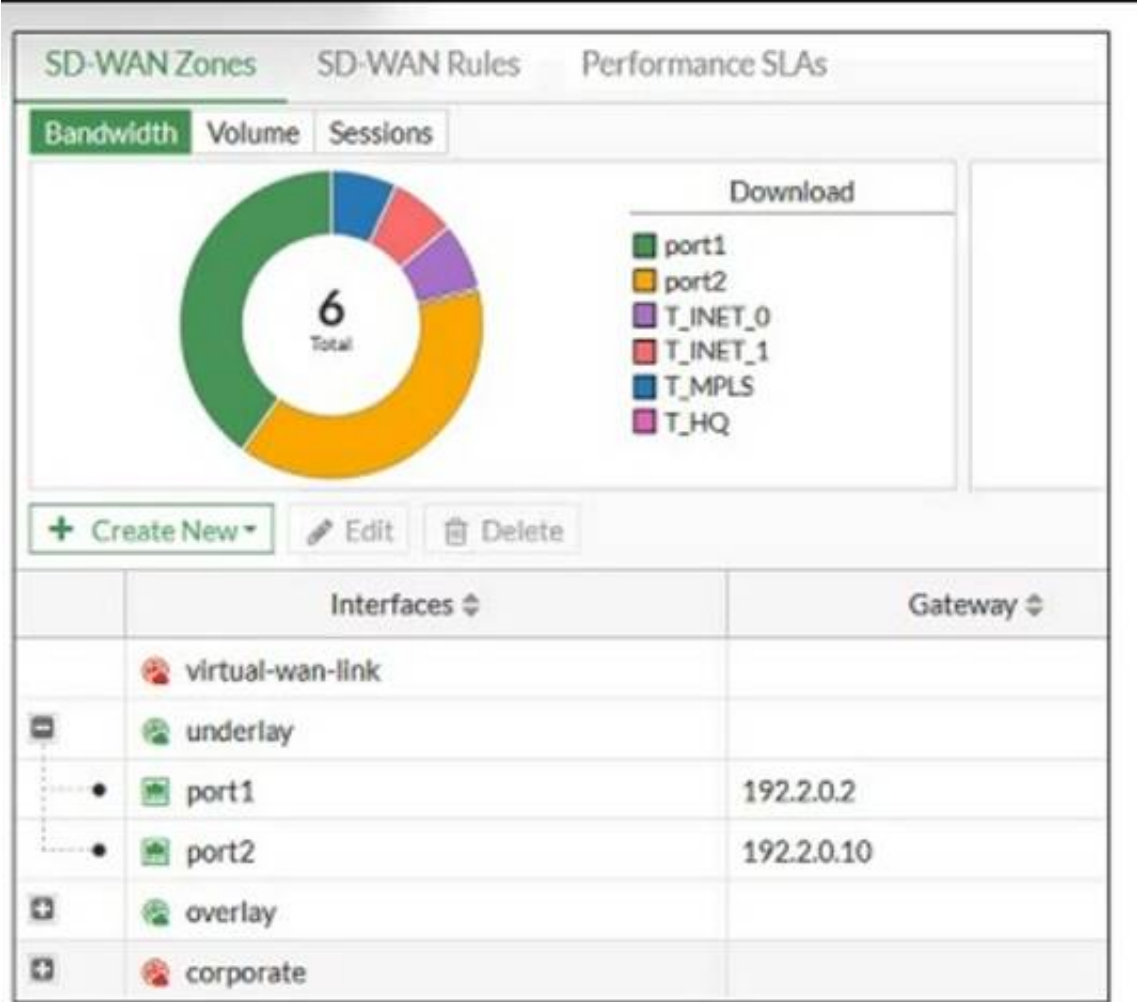
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

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

Answer: AC

NEW QUESTION 47

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 49**

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 53**

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 58**

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 63**

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 65**

Refer to the exhibit.

### Create New SD-WAN Interface Member

|                              |                                     |
|------------------------------|-------------------------------------|
| Sequence Number              | 1                                   |
| Interface Member             |                                     |
| SD-WAN Zone                  | virtual-wan-link                    |
| Gateway IP                   | 0.0.0.0                             |
| Cost                         | 0                                   |
| Status                       | <input checked="" type="checkbox"/> |
| Priority                     | 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 67

Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

- A. get router info routing-table all
- B. diagnose debug application ike
- C. diagnose vpn tunnel list
- D. get ipsec tunnel list

**Answer:** B

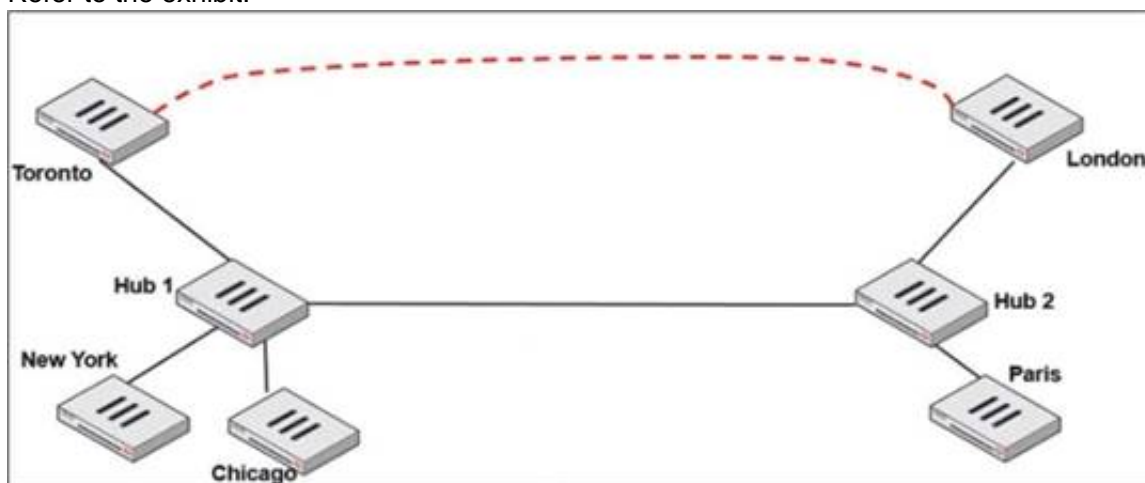
#### Explanation:

IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations.

- diagnose debug console timestamp enable
- diagnose vpn ike log filter clear
- diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
- diagnose debug application ike -1
- diagnose debug enable

#### NEW QUESTION 71

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 75**

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 76**

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 81**

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 83**

.....



## 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](#)**