

Fortinet.NSE7_SDW-7.2.by.Anne.42q

Number: NSE7_SDW-7.2
Passing Score: 800
Time Limit: 120
File Version: 1.0

Website: www.VCEplus.io

Twitter: https://twitter.com/VCE_Plus

Exam Code: NSE7_SDW-7.2

Exam Name: Fortinet NSE 7 - SD-WAN 7.2



Exam A

QUESTION 1

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

Correct Answer: A, D

Section:

QUESTION 2

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.

Correct Answer: C, D

Section:

QUESTION 3

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.

Correct Answer: B

Section:

QUESTION 4

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.

Correct Answer: B

Section:

QUESTION 5

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.

Correct Answer: A, C

Section:

QUESTION 6

Refer to the exhibit.

Create New SD-WAN Interface Member

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

www.VCEplus.io

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

Correct Answer: B, D

Section:

QUESTION 7

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.

Correct Answer: C, D

Section:

www.VCEplus.io

QUESTION 8

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.

Correct Answer: B, D

Section:

QUESTION 9

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.

Correct Answer: B, D, E

Section:

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.

QUESTION 10

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "T_INET_0_0"
    set type dynamic
    set interface "port1"
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route enable
    set psksecret ENC
Zv9n4Urfk0W4jj8vWI+KywxBG4ZDT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW2ZHQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+03CYBMLwkFZmdU6RsT+qvybblVX+Ioy
HK5EXakpmz5RiltELgZ9Gg==
  next
end
```

Which configuration change is required if the responder FortiGate uses a dynamic routing protocol to exchange routes over IPsec?

- A. type must be set to static.
- B. mode-cfg must be enabled.
- C. exchange-interface-ip must be enabled.
- D. add-route must be disabled.

Correct Answer: D

Section:

QUESTION 11

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.

Correct Answer: D

Section:

QUESTION 12

Refer to the exhibit.

www.VCEplus.io


```
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
```

www.VCEplus.io

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

Correct Answer: A, B, D

Section:

QUESTION 13

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.

Correct Answer: B

Section:

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.

Reference: 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.

QUESTION 14

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.

Correct Answer: A, B

Section:

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.

Reference: 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.

QUESTION 15

What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

- A. The FortiGate cloud key has not been added to the FortiGate cloud portal.
- B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
- C. The zero-touch provisioning process has completed internally, behind FortiGate.
- D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
- E. A factory reset performed on FortiGate.

Correct Answer: A, C

Section:

QUESTION 16

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.

Correct Answer: B, C

Section:

QUESTION 17

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->8.8.8.8:8(192.168.73.132:62662)
hook=pre dir=reply act=dnat 8.8.8.8:62662->192.168.73.132:0(10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

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

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

Correct Answer: C

Section:

QUESTION 18

Refer to the exhibits.

www.VCEplus.io

Exhibit A

+ Create New
Edit
Delete

Name
Branch_IPsec_1
Branch_IPsec_2
BRANCH_IPsec_Recomm

+ Create New
Edit
Delete
More

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

+ Create New
Edit
Delete

Name
Branch_IPsec_1
Branch_IPsec_2
BRANCH_IPsec_Recomm

+ Create New
Edit
Delete
More

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

Exhibit B

invalid template assignment - conflicting template assignment scope: device branch1_fgt, vdom root, _ipsec template [Branch_IPsec_1] and [Branch_IPsec_2]

Exhibit A shows two IPsec templates to define Branch_IPsec_1 and Branch_IPsec_2. Each template defines a VPN tunnel. Exhibit B shows the error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device. Which statement best explain the cause for this issue?

- A. You can assign only one template with a tunnel of type static to each FortiGate device
- B. You can define only one IPsec tunnel from branch devices to HUB1.
- C. You can assign only one IPsec template to each FortiGate device.
- D. You should review the branch1_fgt configuration for the already configured tunnel with the name HUB1-VPN2.

Correct Answer: C

Section:

Explanation:

The error message in Exhibit B indicates a conflicting template assignment. This occurs because FortiManager does not allow the assignment of multiple IPsec templates that define VPN tunnels with the same name or settings to the same FortiGate device. The conflict arises from trying to assign a second IPsec template to a device that already has one assigned.

Reference: This is based on Fortinet's best practices and administrative guidelines which state that each FortiGate device should be assigned a unique IPsec template to avoid configuration conflicts.

QUESTION 19

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.

Correct Answer: D

Section:

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. Reference=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.

Reference: 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.

QUESTION 20

Which are three key routing principles in SD-WAN? (Choose three.)

- A. FortiGate performs route lookups for new sessions only.
- B. Regular policy routes have precedence over SD-WAN rules.
- C. SD-WAN rules have precedence over ISDB routes.
- D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
- E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Correct Answer: B, D, E

Section:**Explanation:**

Study Guide 7.2, pages 125, 129, 151

www.VCEplus.io

QUESTION 21

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
orgin->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_uid_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
rpd_b_link_id=ff000002 rpd_b_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.

Correct Answer: D

Section:

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.

QUESTION 22

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

Correct Answer: B, C

Section:

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.

QUESTION 23

Refer to the exhibits.

www.VCEplus.io

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

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

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

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

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

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

Exhibit B

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2		port2

Security	
APP Count	2
Level	notice
General	
Log ID	0000000013
Session ID	769
Tran Display	snat
Virtual Domain	root
Source	
Country	Reserved
Device ID	FGVM01TM22000077
Device Name	branch1_fgt
IP	10.0.1.101
Interface	port5
Interface Role	undefined
NAT IP	192.2.0.9
NAT Port	51042
Port	51042
Source	10.0.1.101
UEBA Endpoint ID	1025
UEBA User ID	3
Destination	
Country	United States
End User ID	3
Endpoint ID	101
Host Name	www.gotomeeting.com
IP	23.212.248.205
Interface	port2

www.VCEplus.io

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.

Correct Answer: A, D

Section:

Explanation:

Study guide 7.2 Page 191

QUESTION 24

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.

Correct Answer: A

Section:

Explanation:

Study Guide 7.2, page 176.

QUESTION 25

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.

Correct Answer: A, D

Section:

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.

QUESTION 26

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 pksecret ENC MXtFGK0xLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73f2pSXS/
jv9oshWeQiNEjOJEtUqqD8mAw7G2ZLT1sR3/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=ntf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag-rtc 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 rxb=1280 txb=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: 0:0.0.0.0-255.255.255.0
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 8547efb42d148c6692fb2af0d01ff12d
ah=sha1 key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6a1f9fe5ab38b953dd4782f
ah=sha1 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
```

www.VCEplus.io

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. Most Voted
- B. The phase 1 configuration supports the network-overlay setting. Most Voted
- C. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
- D. Dead peer detection is disabled.

Correct Answer: A, B

Section:

QUESTION 27

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
```

www.VCEplus.io

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
end
```

www.VCEplus.io

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.

Correct Answer: C

Section:

QUESTION 28

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

Correct Answer: B, C

Section:

Explanation:

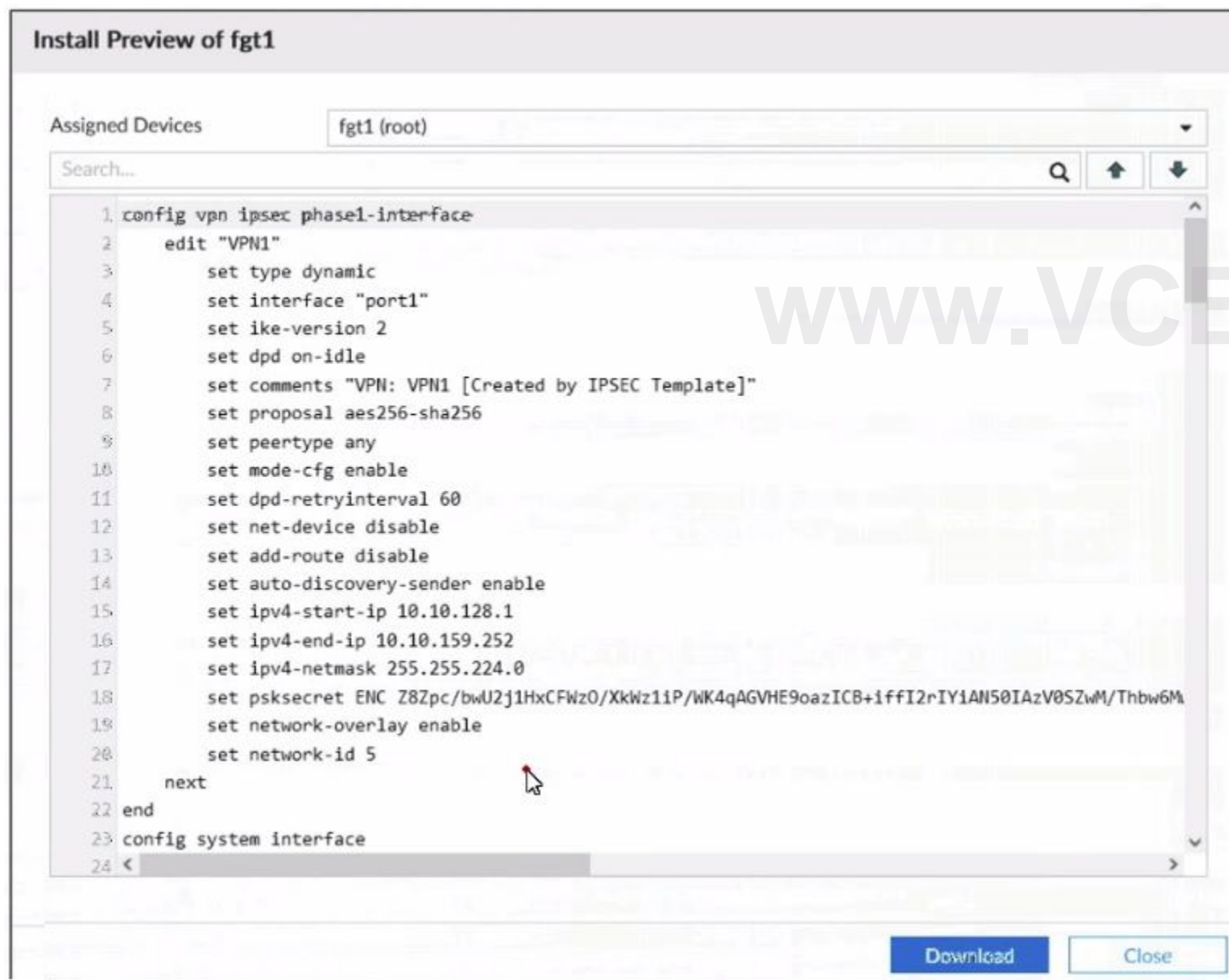
According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:

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.

QUESTION 29

Refer to the exhibit.



An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

- A. It is a hub device. It can send ADVPN shortcut offers.
- B. It is a spoke device that establishes dynamic IPsec tunnels to the hub. The subnet range is 10.10.128.0/23.
- C. It is a spoke device that establishes dynamic IPsec tunnels to the hub. It can send ADVPN shortcut requests.
- D. It is a hub device and will automatically discover the spoke devices that are in the SD-WAN topology.

Correct Answer: C

Section:

Explanation:

According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:

type: dynamic for spokes, static for hubs

interface: the WAN interface to use for the IPsec tunnel

network-overlay: enable for spokes, disable for hubs

network-id: a unique identifier for each spoke

auto-discovery-sender: enable for hubs, disable for spokes

auto-discovery-receiver: enable for spokes, disable for hubs

Based on the exhibit, the FortiGate device has the following configuration:

type: dynamic

interface: port1

network-overlay: enable

network-id: 5

auto-discovery-sender: disable

auto-discovery-receiver: enable

Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

www.VCEplus.io

QUESTION 30

Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

- A. Type of physical link connection
- B. Internet service database (ISDB) address object
- C. Source and destination IP address
- D. URL categories
- E. Application signatures

Correct Answer: A, B, E

Section:

QUESTION 31

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

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

Correct Answer: B, D

Section:

QUESTION 32

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

Correct Answer: A

Section:

QUESTION 33

Refer to the exhibits.

Exhibit A -

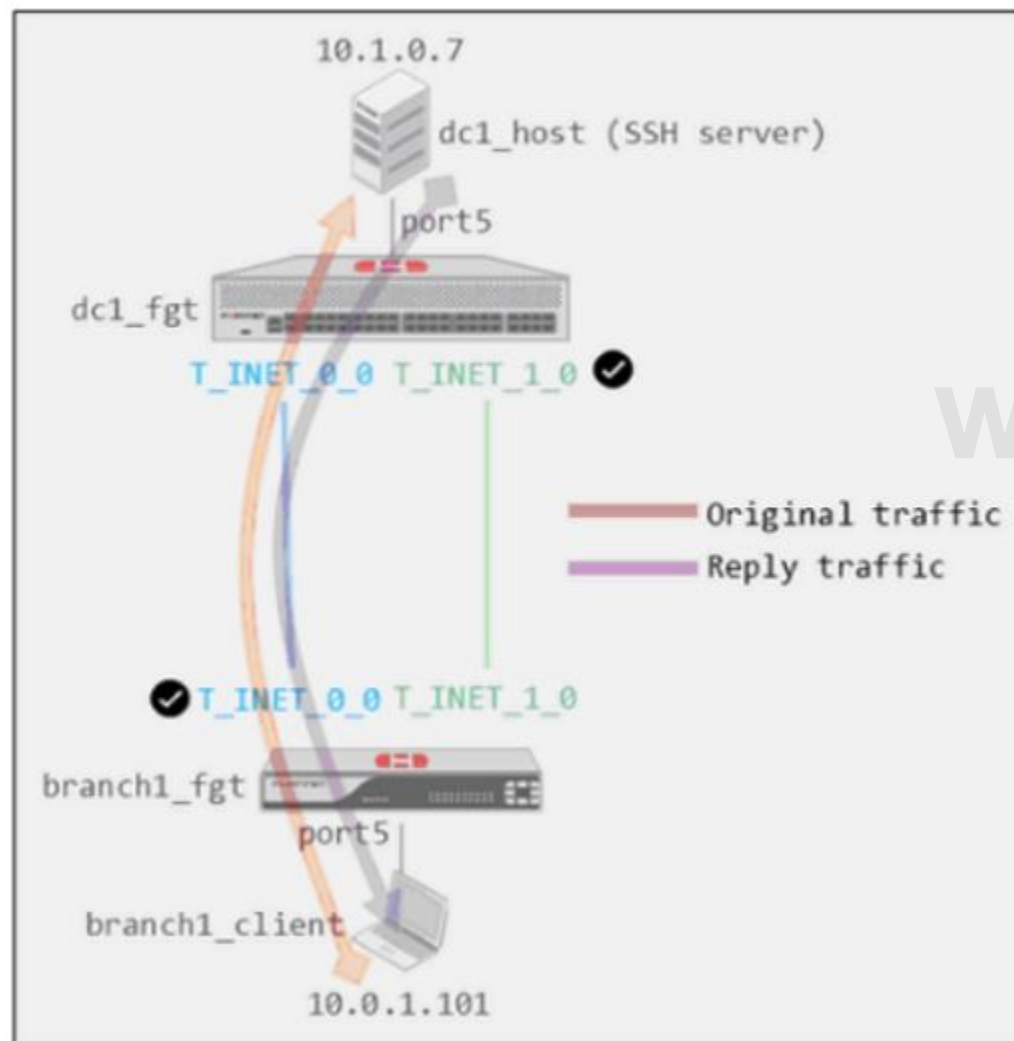


Exhibit B -

```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt.

When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

- A. Enable auxiliary-session under config system settings.
- B. Disable tcp-session-without-syn under config system settings.
- C. Enable snat-route-change under config system global.
- D. Disable allow-subnet-overlap under config system settings.

Correct Answer: B

Section:

QUESTION 34

Refer to the exhibit.

www.VCEplus.io

```
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.

Correct Answer: A

Section:

QUESTION 35

What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

- A. The ISDB is dynamically updated and reduces administrative overhead.
- B. The ISDB requires application control to maintain signatures and perform load balancing.
- C. The ISDB applies rules to traffic from specific sources, based on application type.
- D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Correct Answer: A, D

Section:

QUESTION 36

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.

Correct Answer: D

Section:

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.

QUESTION 37

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

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

Correct Answer: A, C

Section:

QUESTION 38

Exhibit.

```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The exhibit shows the output of the command `diagnose sys sdwan health-check status` collected on a FortiGate device. Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

- A. The health-check VPN_PING orders the members according to the lowest jitter.

- B. The interface T_INET_1 missed one SLA target.
- C. There is no SLA criteria configured for the health-check Level3_DNS.
- D. The interface T_INET_0 missed three SLA targets.

Correct Answer: A, C

Section:

Explanation:

According to the FortiGate / FortiOS 6.4.2 Administration Guide, the health check status command displays the status of the health check probes for each SD-WAN member interface. The output includes the following information:

state: the current state of the interface, either alive or dead

packet-loss: the percentage of packets lost during the health check

latency: the average round-trip time in milliseconds

jitter: the variation in latency

mos: the mean opinion score, a measure of voice quality

bandwidth: the available bandwidth in kilobits per second for each direction (up, down, bi)

sla map: a bitmap that indicates which SLA criteria are met or failed

Based on the exhibit, the following statements are correct:

The health-check VPN_PING orders the members according to the lowest jitter. This means that the interface with the lowest jitter value is listed first, followed by the next lowest, and so on. In the exhibit, the order is T_MPLS, T_INET_1, and T_INET_0.

There is no SLA criteria configured for the health-check Level3_DNS. This means that the health check does not use any SLA parameters to determine the state of the interface. In the exhibit, the sla map value is 0x0 for both port1 and port2, indicating that no SLA criteria are applied.

QUESTION 39

Refer to the exhibits.

Exhibit A

```
branch1_fgt (3) # show
config service
  edit 3
    set name "Corp"
    set mode sla
    set dst "Corp-net"
    set src "LAN-net"
    config sla
      edit "VPN_PING"
        set id 1
      next
      edit "VPN_HTTP"
        set id 1
      next
    end
    set priority-members 3 4 5
    set gateway enable
  next
end
```

Exhibit B -

www.VCEplus.io

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(2):
  1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
  2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), 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 # get router info routing-table all | grep T_
S      10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
          [1/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S      10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5

branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4 , gateway: 172.16.1.5, peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status. The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

- A. The traffic will be load balanced across all three overlays.
- B. The traffic will be routed over T_INET_0_0.
- C. The traffic will be routed over T_MPLS_0.
- D. The traffic will be routed over T_INET_1_0.

Correct Answer: D

Section:

QUESTION 40

Refer to the exhibit.

+ 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	naft.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	13	l2t.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_ts	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.

Correct Answer: B

Section:

QUESTION 41

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

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

Correct Answer: C, D

Section:

QUESTION 42

Refer to the exhibits.

www.VCEplus.io

Exhibit A

<pre> 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 </pre>
<pre> 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): </pre>
<pre> 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 </pre>

Exhibit B

<pre> 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 </pre>
--

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.

Correct Answer: A, D

Section: