Vendor: Fortinet

Exam Code: FCSS_SDW_AR-7.4

Exam Name: FCSS - SD-WAN 7.4 Architect

Version: DEMO

QUESTION 1
You manage an SD-WAN topology. You will soon deploy 50 new branches.

Which three tasks can you do in advance to simplify this deployment? (Choose three.)

A. Update the DHCP server configuration.
B. Create model devices.
C. Create a ZTP template.
D. Define metadata variables value for each device.
E. Create policy blueprint.

Answer: BCE
Explanation:
Creating a ZTP (Zero Touch Provisioning) template automates onboarding of new branches.

Policy blueprints allow predefining consistent configurations for security and SD-WAN rules.

Model devices help preconfigure settings tied to device models, speeding up deployment.

QUESTION 2
You are planning a new SD-WAN deployment with the following criteria:

```
- Two regions
- Most of the traffic is expected to remain within its region
- No requirement for inter-region ADVPN
```

To remain within the recommended best practices, which routing protocol should you select for the overlays?

A. OSPF for the routing within each region and EBGP between the regions.
B. IBGP with BGP on loopback within each region and EBGP between the regions.
C. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.
D. IBGP within each region and between the regions.

Answer: B
Explanation:
Using iBGP with BGP on loopback within each region ensures scalable and stable routing inside the region, while eBGP between regions aligns with best practices to maintain clear boundaries, reduce convergence complexity, and support region separation.

QUESTION 3
Refer to the exhibit. The administrator configured the IPsec tunnel VPN1 on a FortiGate device with the parameters shown in exhibit.
Based on the configuration, which three conclusions can you draw about the characteristics and requirements of the VPN tunnel? (Choose three.)

```
config vpn ipsec phase1-interface
     edit "VPN1"
          set interface "port1"
          set ike-version 2
          set peertype any
          set exchange-interface-ip enable
          set mode-cfg disable
          set proposal aes256-sha256
          …
     end
end
```

A. The tunnel interface IP address on the spoke side is provided by the hub.
B. The remote end can be a third-party IPsec device.
C. The administrator must manually assign the tunnel interface IP address on the hub side
D. The remote end must support IKEv2.
E. This configuration allows user-defined overlay IP addresses.

Answer: BCD
Explanation:
set peertype any allows interoperability with third-party IPsec devices.

set ike-version 2 requires the remote peer to support IKEv2.

set mode-cfg disable means no IP address will be pushed, so the hub must assign the interface IP manually.

QUESTION 4
You have a FortiGate configuration with three user-defined SD-WAN zones and two members in each of these zones. One SD-WAN member is no longer in use in health-check and SD-WAN rules. You want to delete it.
What happens if you delete the SD-WAN member from the FortiGate GUI?

A. FodiGate accepts the deletion and removes routes as required.
B. FortiGate displays an error message. You must use the CLI to delete an SD-WAN member.
C. FortiGate displays an error message. SD-WAN zones must contain at least two members
D. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: A
Explanation:
In FortiOS, you can remove an SD-WAN member from the GUI as long as it is not in use in any health-checks, SD-WAN rules, or policies.

When you delete it, FortiGate will automatically clean up related routes (static or dynamic SD-WAN routes referencing that member).

QUESTION 5

Refer to the exhibits. The exhibits show the source NAT (SNAT) global setting. port2 interface settings, and the routing table on FortiGate.
The administrator increases the member priority on port2 to 20. Upon configuration changes and the receipt of new packets, which two actions does FortiGate perform on existing sessions established over port2? (Choose two.)

Global System configuration

```
config system global
     set snat-route-change enable
end
```

Interface port2 configuration

```
config system interface
     [...]
     edit "port2"
          set vdom "root"
          set mode dhcp
          set type physical
          set snmp-index 2
     next
     [...]
```

Routing Table on FortiGate

```
branch1_fgt # get router info routing-table all
Codes: K – kernel, C – connected, S – static, R – RIP, B – BGP
       O – OSPF, IA – OSPF inter area
       N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
       E1 – OSPF external type 1, E2 – OSPF external type 2
       i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area
       * – candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
                  [1/0] via 192.2.0.10, port1, [10/0]

...
```

A. FortiGate continues routing all existing sessions over port2.
B. FortiGate routes only new sessions over port2.
C. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
D. FortiGate flags the sessions as dirty.

E. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: DE
Explanation:
With set snat-route-change enable, FortiGate updates SNAT sessions' egress interface and gateway if a better route becomes available (e.g., port1 after priority change).

The sessions are flagged as dirty, meaning their routing and SNAT details are refreshed upon new traffic matching the session.

QUESTION 6
Refer to the exhibit. The exhibit shows the health-check configuration on a FortiGate device used as a spoke. You notice that the hub FortiGate doesn't prioritize the traffic as expected.

Which two configuration elements should you check on the hub? (Choose two.)

```
config system sdwan
     config health_check
          edit "DNS"
               set server "4.2.2.1" "4.2.2.2"
               set detect-mode active
               set protocol ping
               set embed-measured-health enable
               set members 3 4
               config sla
                    edit 1
                    set link-cost-factor latency
                    set latency-threshold 100
               end
          next
     end
end
```

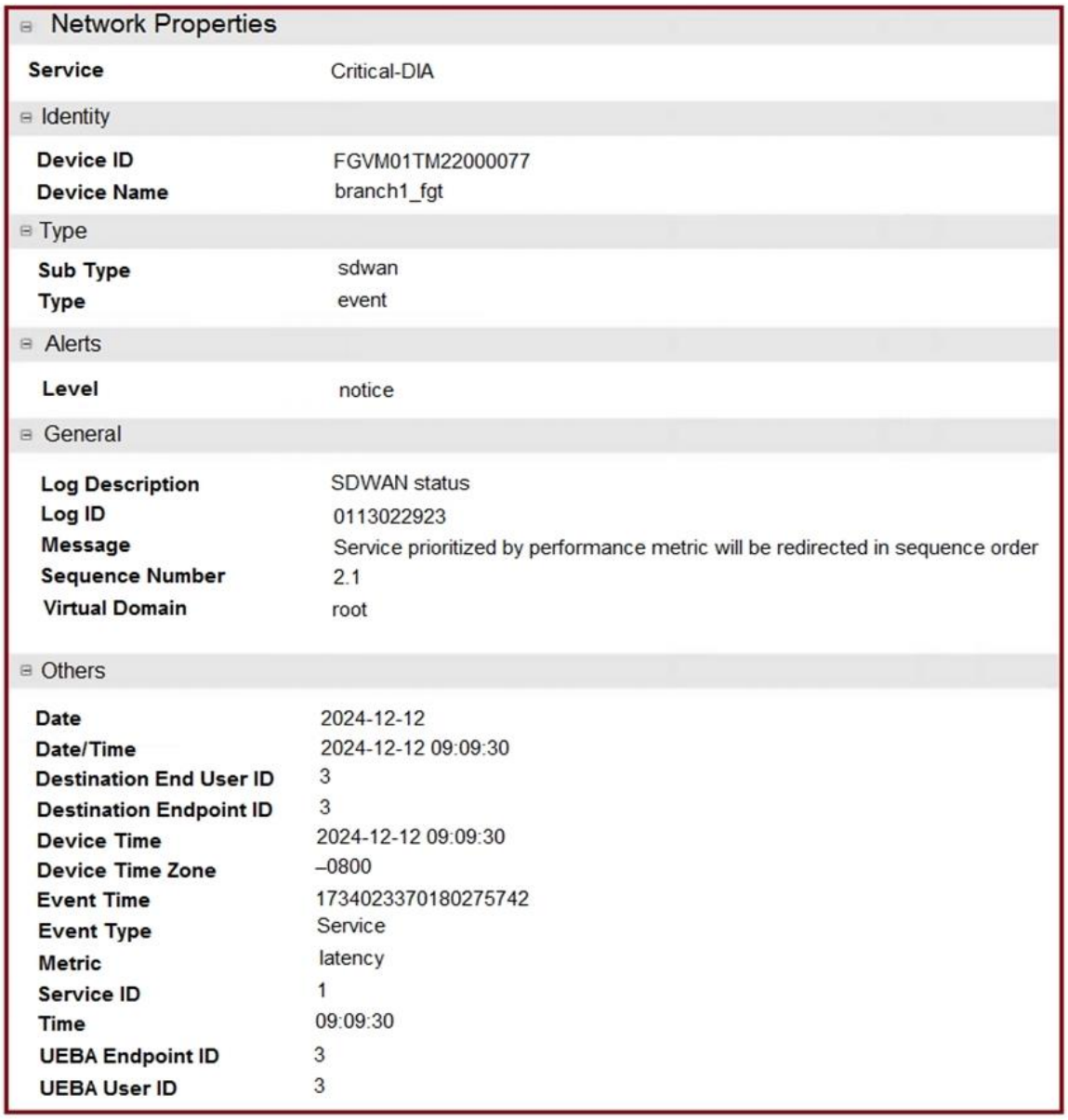
A. The performance SLA has the parameter `priority-out-sla` configured.
B. This performance SLA uses the same members.
C. The performance SLA uses the same criteria.
D. The performance SLA is configured with set `embedded-measure accept`.

Answer: CD
Explanation:
The hub must use a performance SLA with the same criteria as the spoke's health check. The spoke's health check is using ping (protocol ping) and measuring latency (link-cost-factor latency). For the hub to use the data sent by the spoke, its performance SLA must be configured to measure the same metrics. If the hub is looking for jitter or packet loss, it will not use the latency data sent by the spoke.

When a spoke sends embedded health data, the hub FortiGate must be configured to receive and use it. This is done by setting set embedded-measure accept within the performance SLA configuration on the hub. This setting explicitly tells the hub to trust and use the performance metrics received from the remote FortiGate (the spoke). Without this setting, the hub will likely ignore the embedded health data and rely on its own health checks, which could lead to incorrect traffic prioritization.

QUESTION 7
Refer to the exhibits. The exhibits show an SD-WAN event log, the member status, and the SD-WAN rule configuration.

Which two conclusions can you draw from the information shown? (Choose two.)



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	2024-12-12
Date/Time	2024-12-12 09:09:30
Destination End User ID	3
Destination Endpoint ID	3
Device Time	2024-12-12 09:09:30
Device Time Zone	–0800
Event Time	1734023370180275742
Event Type	Service
Metric	latency
Service ID	1
Time	09:09:30
UEBA Endpoint ID	3
UEBA User ID	3

SD-WAN member status

```
branch1_fgt # diagnose sys sdwan member
Member(1): transport-group: 0, interface: port1, flags=0x0,
gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): transport-group: 0, interface: port2, flags=0x0,
gateway: 192.2.0.10, source 192.2.0.9, priority: 10 1024, weight: 0
```

SD-WAN rule configuration

```
config service
     edit 1
          set name "Critical-DIA"
          set mode priority
          set src "LAN-net"
          set internet-service enable
          set internet-service-app-ctrl 41469 16920
          set internet-service-app-ctrl-category 28
          set health-check "Corp_HC"
          set priority-members 1 2
     next
end
```

A. The administrator configured the service ID 1 with the highest priority member for port2.
B. Port2 has a lower latency than port1.
C. FortiGate updated the outgoing interface list on the rule so it prefers port2.
D. The administrator configured the SD-WAN rule ID 1 with the default strategy mode.

Answer: BC
Explanation:
The SD-WAN rule (config service edit 1) is configured with set mode priority. This means the rule selects the best interface based on a defined performance metric, as opposed to a simple static priority or SLA. The event log (image_41cfb5.png) shows Metric latency and Message Service prioritized by performance metric will be redirected in sequence order. This indicates that the rule is using latency to determine the preferred member. Given that the log message is about a change, and the most logical reason for a change in a priority mode is that a different member is now the best performer, it implies that the latency on port2 has become lower than that on port1.

The log message Service prioritized by performance metric will be redirected in sequence order confirms that FortiGate is changing the member being used for this service. Because the mode is priority, FortiGate dynamically selects the member that currently meets the best performance criteria, which in this case is latency. The log implies a new member has been selected as the most optimal, and with the default configuration, the members are sorted based on their performance, so the outgoing interface list is effectively updated to prefer the new best-performing member (port2).

QUESTION 8
Which three factors about SLA targets and SD-WAN rules should you consider when configuring

SD-WAN rules? (Choose three.)

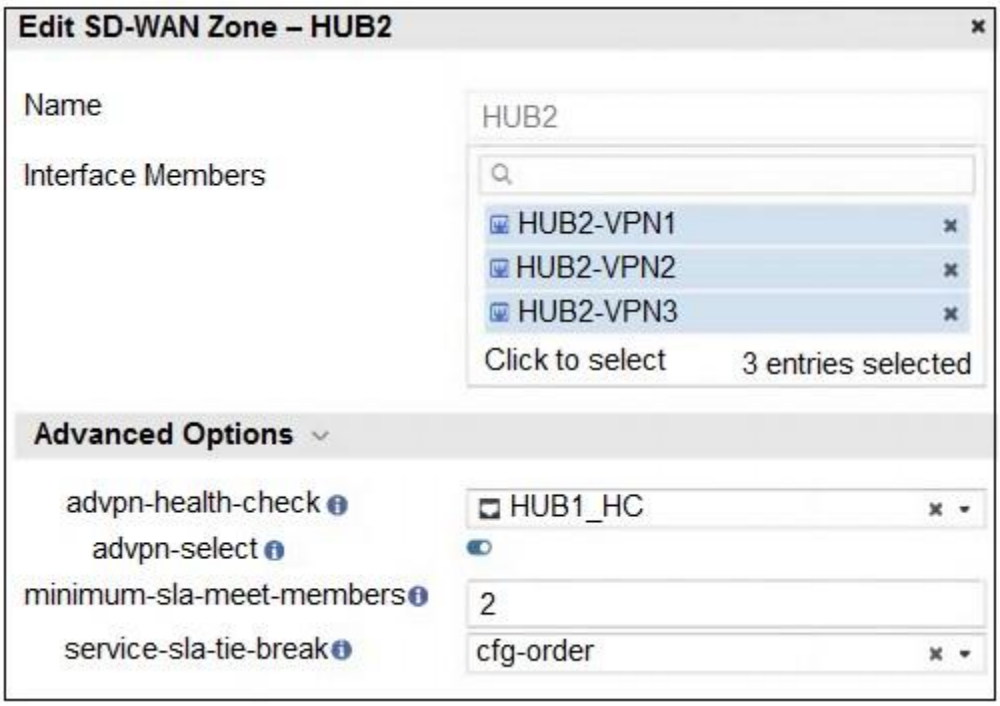
A. Member metrics are measured only if a rule uses the SLA target.
B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.
C. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.
D. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.
E. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.

Answer: BCE
Explanation:
The use of SLA targets is specific to certain SD-WAN strategies. The "Lowest Cost (SLA)" and "Maximize Bandwidth (SLA)" strategies are explicitly designed to use the configured SLA targets to make routing decisions. The "Best Quality" strategy uses performance metrics but does not necessarily require or reference SLA targets in the same way, while "Manual" does not use metrics at all for path selection.

This is a core function of SD-WAN rules with SLA targets. The purpose of configuring an SLA target with specific thresholds for latency, jitter, and packet loss is to define what is considered "acceptable" performance for an application. SD-WAN rules then use these targets to check if the members (interfaces) meet these requirements before a flow is steered over them, ensuring that a preferred path still offers a good user experience.

FortiGate allows for a single SD-WAN rule to reference multiple, different performance SLAs. This is crucial for complex deployments where a single SD-WAN rule needs to handle traffic for multiple applications that have distinct performance requirements. For example, a single rule might direct VoIP traffic based on one performance SLA with strict latency/jitter targets, while simultaneously handling general web traffic using another performance SLA with more lenient requirements.

QUESTION 9
Refer to the exhibit that shows an SD-WAN zone configuration on the FortiManager GUI.



Based on the exhibit, how will the FortiGate device behave after it receives this configuration?

A. The configuration instructs FortiGate to choose an ADVPN shortcut based on SD-WAN information.
B. The configuration instructs FortiGate to allow ADVPN shortcuts for the tunnels of this SD-WAN zone.
C. The configuration instructs FortiGate to establish shortcuts only when at least two members meet the SLA target.
D. The configuration instructs FortiGate to establish shortcuts only for overlay interfaces that meet the SLA target HUB1_HC.

Answer: C
Explanation:
This is because the setting minimum-sla-meet-members = 2 requires at least two SD-WAN zone members (in this case, HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3) to pass the defined SLA health check (HUB1_HC) before the FortiGate will establish ADVPN shortcuts. If fewer than two members meet the SLA, shortcuts will not be created.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14