Fortinet

Exam Questions NSE5_SSE_AD-7.6

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator

NEW QUESTION 1
Which statement about security posture tags in FortiSASE is correct?

A. Multiple tags can be assigned to an endpoint, but only one is used for evaluation.
B. Multiple tags can be assigned to an endpoint and used for evaluation.
C. Tags are static and do not change with endpoint status.
D. Only one tag can be assigned to an endpoint.

Answer: B

NEW QUESTION 2
A FortiGate device is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.
What must you do as part of this configuration update process? (Choose one answer)

A. Replace references to interfaces used as SD-WAN members in the firewall policies.
B. Replace references to interfaces used as SD-WAN members in the routing configuration.
C. Disable the interface that you want to use as an SD-WAN member.
D. Purchase and install the SD-WAN license, and reboot the FortiGate device.

Answer: A

NEW QUESTION 3
You are configuring SD-WAN to load balance network traffic. Which two facts should you consider when setting up SD-WAN? (Choose two.)

A. When applicable, FortiGate load balances traffic through all members that meet the SLA target.
B. SD-WAN load balancing is possible only when using the manual and the best quality strategies.
C. Only the manual and lowest cost (SLA) strategies allow SD-WAN load balancing.
D. You can select the outsessions hash mode with all strategies that allow load balancing.

Answer: AD

NEW QUESTION 4
An SD-WAN member is no longer used to steer SD-WAN traffic. You want to update the SD-WAN configuration and delete the unused member.
Which action should you take first? (Choose one answer)

A. Move the SD-WAN member to the virtual-wan-link zone.
B. Disable the interface.
C. Remove the member from the performance service-level agreement (SLA) definitions.
D. Delete static route definitions for that interface.

Answer: C

NEW QUESTION 5
Refer to the exhibit.

Diagnose output

```
fgt_1 # diagnose  sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
 link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.906, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.079, selected
  Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla
hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HQ_T1 overlay), alive, sla(0x3), gid(0), cfg_order(0),
local cost(0), selected
    2: Seq_num(5 HQ_T2 overlay), alive, sla(0x3), gid(0), cfg_order(1),
local cost(0), selected
    3: Seq_num(6 HQ_T3 overlay), alive, sla(0x3), gid(0), cfg_order(2),
local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

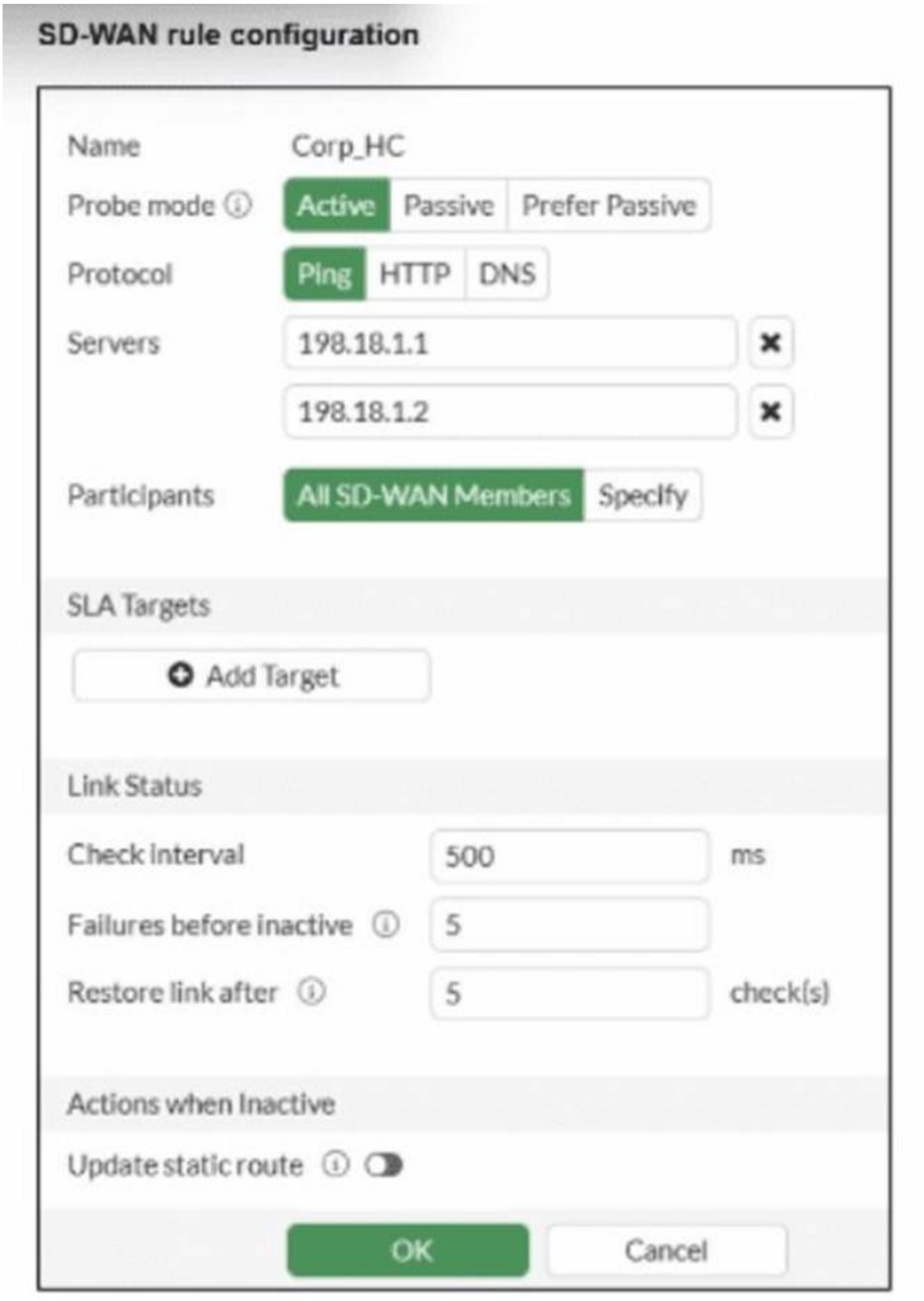
The exhibit shows output of the command diagnose sys sdwan service collected on a FortiGate device.
The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the social media application Facebook.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.
B. There is no service defined for the Facebook application, so FortiGate applies servicerule 3 and directs the traffic to headquarters.
C. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1, HQ_T2, HQ_T3.
D. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.

Answer: AC

Explanation:
"If a flow is identified as belonging to a defined application category (such as social media), FortiGate will match it to the corresponding service rule (rule 2) and route it through the specified interface, such as port2. However, if the application is not recognized during the session setup, the system defaults to load balancing the traffic using the available tunnels according to the policy for unclassified traffic, ensuring continuous connectivity while waiting for application classification." This guarantees both performance and resilience.

NEW QUESTION 6
Refer to the exhibit.

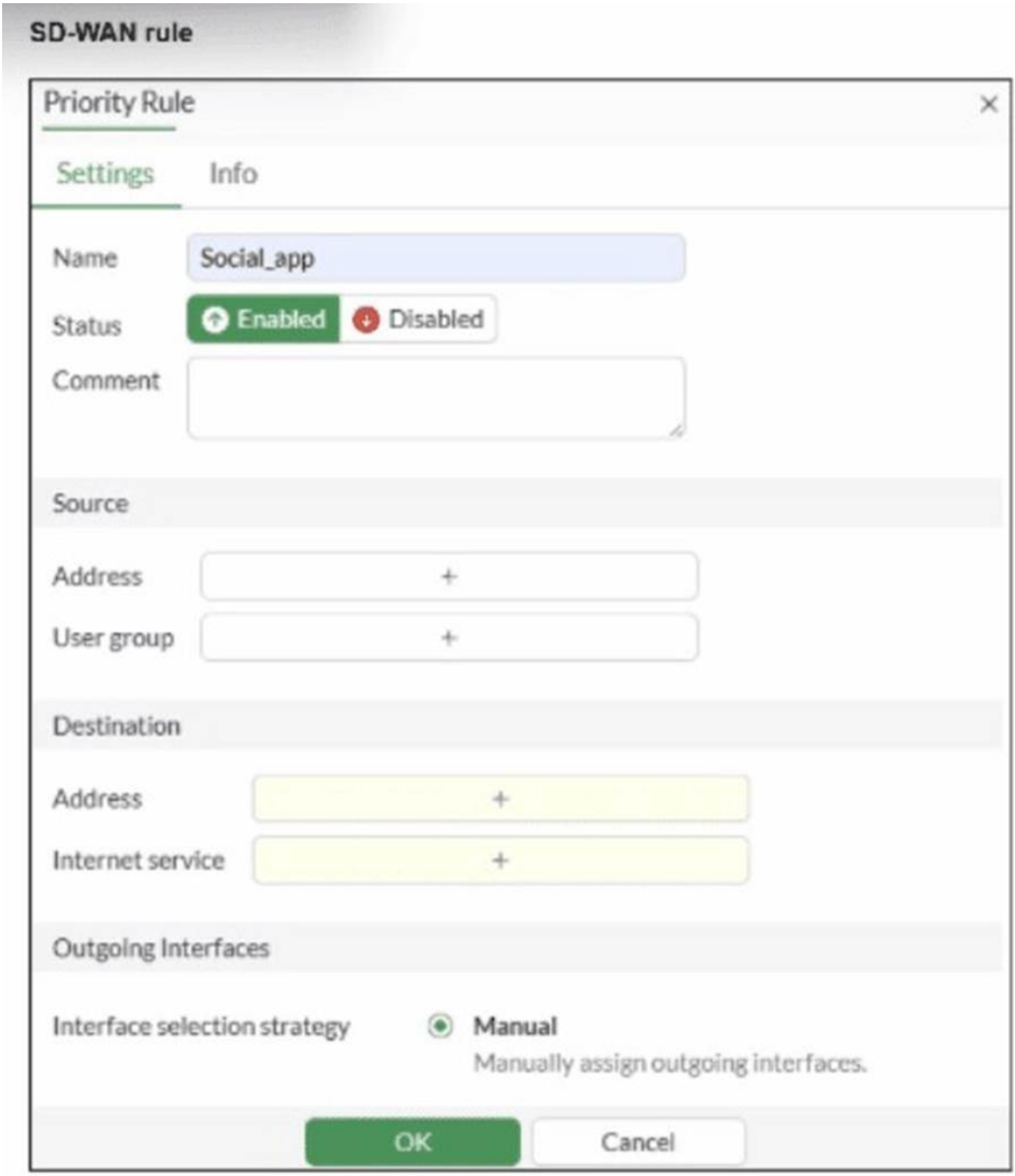


You want the performance service-level agreement (SLA) to measure the jitter of each member. Which configuration change must you make to achieve this result?

A. No change is required.
B. Add an SLA target and define a jitter threshold.
C. Specify the participant members.
D. Set the protocol to HTTP.

Answer: A

NEW QUESTION 7
Refer to the exhibit.

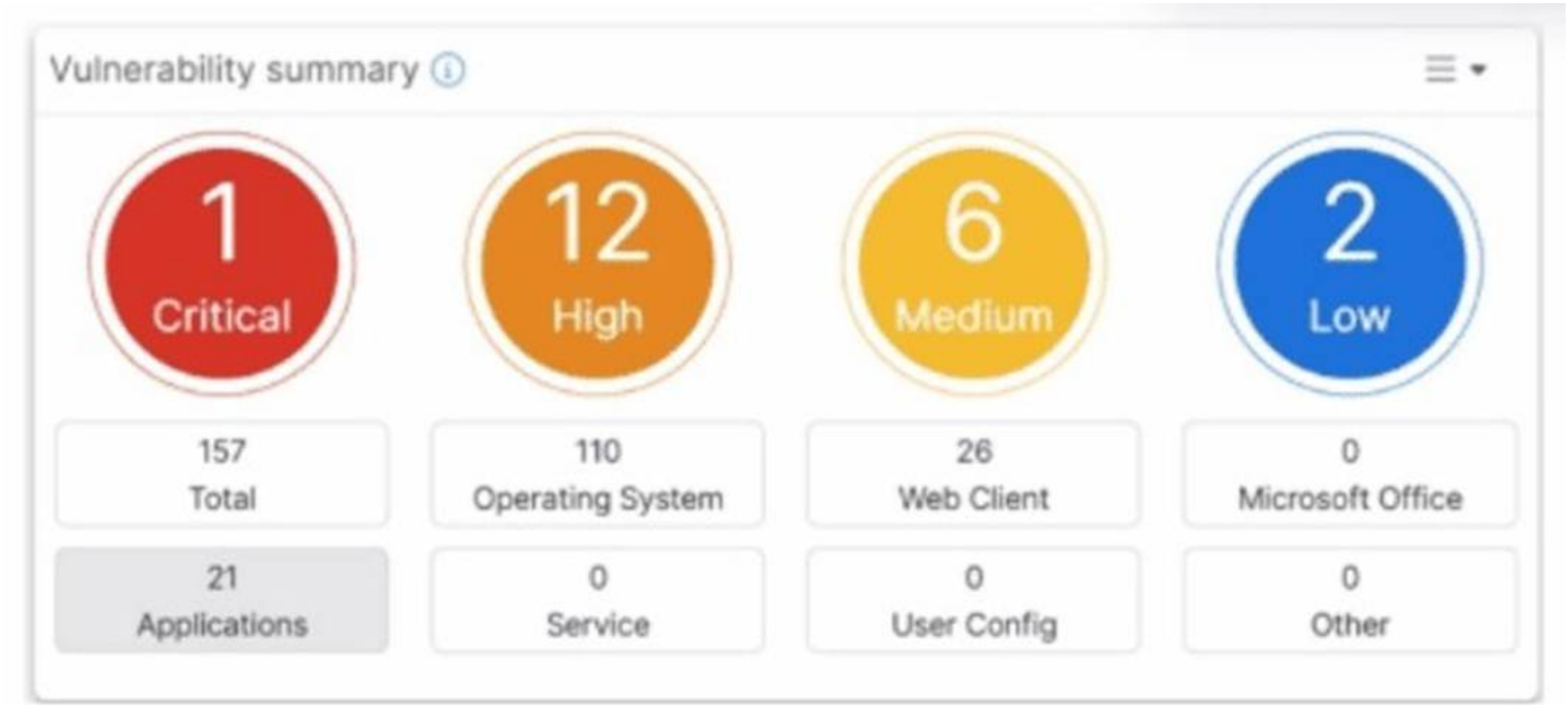


You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link. What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

A. Install a license to allow applications as destinations of SD-WAN rules.
B. In the Internet service field, select Facebook and LinkedIn.
C. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.
D. Enable the visibility of the applications field as destinations of the SD-WAN rule.

Answer: B

NEW QUESTION 8
Refer to the exhibit.



Which two statements about the Vulnerability summary dashboard in FortiSASE are correct? (Choose two.)

A. The dashboard shows the vulnerability score for unknown applications.
B. Vulnerability scan is disabled in the endpoint profile.
C. The dashboard allows the administrator to drill down and view CVE data and severity classifications.
D. Automatic vulnerability patching can be enabled for supported applications.

Answer: CD

NEW QUESTION 9
Which three FortiSASE use cases are possible? (Choose three answers)

A. Secure Internet Access (SIA)
B. Secure SaaS Access (SSA)
C. Secure Private Access (SPA)
D. Secure VPN Access (SVA)
E. Secure Browser Access (SBA)

Answer: ABC

NEW QUESTION 10
You want FortiGate to use SD-WAN rules to steer ping local-out traffic. Which two constraints should you consider? (Choose two.)

A. You must configure each local-out feature individually to use SD-WAN.
B. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
D. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.

Answer: AB

NEW QUESTION 10
Refer to the exhibit

Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local 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


fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd  may_child, gateway: 100.64.1.1,
peer: 192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd  may_child, gateway: 100.64.1.9,
peer: 192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd  may_child, gateway: 172.16.1.5,
peer: 192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0


fgt_A # get router info routing-table all | grep HUB1
S       10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42, [1/0]
```

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 HUB1-VPN1. However, the traffic is routed over HUB1-VPN3.
Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

A. HUB1-VPN1 does not have a valid route to the destination.
B. HUB1-VPN3 has a higher member configuration priority than HUB1-VPN1.
C. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.
D. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device.

Answer: AC

NEW QUESTION 11
SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements must you configure before FortiGate can steer traffic
according to SD-WAN rules? (Choose three.)

A. Firewall policies
B. Security profiles
C. Interfaces
D. Routing
E. Traffic shaping

Answer: ACD

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, for the FortiGate SD-WAN engine to successfully steer traffic using SD-WAN rules, three fundamental configuration components must be in place. This is because the SD-WAN rule lookup occurs only after certain initial conditions are met in the packet flow:
Interfaces (Option C):You must first define the physical or logical interfaces (such as ISP links, LTE, or VPN tunnels) asSD-WAN members. These members are then typically grouped intoSD-WAN Zones. Without designated member interfaces, there is no "pool" of links for the SD-WAN rules to select from.
Routing (Option D):For a packet to even be considered by the SD-WAN engine, there must be a matching route in theForwarding Information Base (FIB). Usually, this is a static route where the destination is the network you want to reach, and the gateway interface is set to theSD-WAN virtual interface(or a specific SD-WAN zone). If there is no route pointing to SD-WAN, the FortiGate will use other routing table entries (like a standard static route) and bypass the SD-WAN rule-based steering logic entirely.
Firewall Policies (Option A):In FortiOS, no traffic is allowed to pass through the device unless aFirewall Policypermits it. To steer traffic, you must have a policy where theIncoming Interfaceis the internal network and theOutgoing Interfaceis the SD-WAN zone (or the virtual-wan-link). The SD-WAN rule selection happens during the "Dirty" session state, which requires a policy match to proceed with the session creation.
Why other options are incorrect:
Security Profiles (Option B):While mandatory forApplication-levelsteering (to identify L7 signatures), basic SD-WAN steering based on IP addresses, ports, or ISDB objects does not require security profiles to be active.
Traffic Shaping (Option E):This is an optimization feature used to manage bandwidth once steering is already determined; it is not a prerequisite for the steering engine itself to function.

NEW QUESTION 13
Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

A. Subnet is the only destination type that supports the Apply condition
B. Apply condition allows split tunneling destinations to ae applied to On-ne
C. off-ne
D. or both types of endpoints
E. You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet
F. Apply condition can be set only to On-net or Off-ne
G. but not both

Answer: BC

Explanation:
According to theFortiSASE 7.6 Feature Administration Guide, steering bypass destinations (also known as split tunneling) allow administrators to optimize bandwidth by redirecting specific trusted traffic away from the SASE tunnel to the endpoint's local physical interface.
Destination Types (Option C): When creating a bypass destination, administrators can select from four distinct types:Infrastructure(pre-defined apps like Zoom/O365),FQDN(specific domains),Local Application(identifying processes on the laptop), orSubnet(specific IP ranges).
Apply Condition (Option B): The "Apply" condition is a flexible setting that allows the administrator to choose when the bypass is active. It can be applied to endpoints that areOn-net(inside the office),Off-net(remote), orBoth. This ensures that if a user is in the office, they don't use the SASE tunnel for local resources, but if they are home, they might still bypass high-bandwidth sites like YouTube to preserve tunnel capacity.
Why other options are incorrect:
Option A: Subnet is one of four types and is not the only type supporting these conditions.
Option D: The system explicitly supports "Both" to ensure consistency across network transitions.

NEW QUESTION 17
Which two delivery methods are used for installing FortiClient on a user's laptop? (Choose two.)

A. Use zero-touch installation through a third-party application store.
B. Download the installer directly from the FortiSASE portal.
C. Send an invitation email to selected users containing links to FortiClient installers.
D. Configure automatic installation through an API to the user's laptop.

Answer: BC

NEW QUESTION 22
Which three reports are valid report types in FortiSASE? (Choose three.)

A. Web Usage Summary Report
B. Endpoint Compliance Deviation Report
C. Vulnerability Assessment Report
D. Shadow IT Report
E. Cyber Threat Assessment

Answer: ACD

NEW QUESTION 27
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE5_SSE_AD-7.6 Practice Exam Features:

* NSE5_SSE_AD-7.6 Questions and Answers Updated Frequently

* NSE5_SSE_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_SSE_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_SSE_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year