Fortinet

Exam Questions NSE5_SSE_AD-7.6

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

NEW QUESTION 1
For a small site, an administrator plans to implement SD-WAN and ensure high network availability for business-critical applications while limiting the overall cost and the cost of pay-per-use backup connections.
Which action must the administrator take to accomplish this plan?

A. Use a mid-range FortiGate device to implement standalone SD-WAN.
B. Implement dynamic routing.
C. Set up a high availability (HA) cluster to implement standalone SD-WAN.
D. Configure at least two WAN links.

Answer: D

NEW QUESTION 2
Refer to the exhibits.

SD-WAN event logs

Identity
Device ID FGVM02TM25002088
Device Name branch1_fgt
Type
Sub Type sdwan
Type event
Alerts
Action
Level notice
General
Log Description SDWAN status
Log ID 0113022923
Member 1
Message Member status changed. Member out-of-sla.
Virtual Domain root
Others
Date 2025-07-01
Date/Time 2025-07-01 05:00:25
Destination End User ID 3
Destination Endpoint ID 3
Destination Geo ID 0
Device Time 2025-07-01 05:00:25
Device Time Zone -0700
Event Time 2025-07-01 05:00:25
Event Type Health Check
Health Check Corp_HC
Log Flag 0
SLA Target ID 1
Source City Sunnyvale

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

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
    edit "Corp_HC"
        set server "198.18.1.1" "198.18.1.2"
        set member 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    end
```

Identity
Device ID FGVM02TM25002088
Device Name branch1_fgt
Type
Sub Type sdwan
Type event
Alerts
Action
Level notice
General
Log Description SDWAN status
Log ID 0113022923
Message Number of pass member changed.
Virtual Domain root
Others
Date 2025-07-01
Date/Time 2025-07-01 05:00:25
Destination End User ID 3
Destination Endpoint ID 3
Destination Geo ID 0
Device Time 2025-07-01 05:00:25
Device Time Zone -0700
Event Time 2025-07-01 05:00:25
Event Type Health Check
Health Check Corp_HC
Log Flag 0
New Value 1
Old Value 2

Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown. Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? (Choose one answer)

A. FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.
B. FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.
C. FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.
D. FortiGate skips SD-WAN rule ID 1.

Answer: C

NEW QUESTION 3
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 4
Which secure internet access (SIA) use case minimizes individual endpoint configuration? (Choose one answer)

A. Agentless remote user internet access
B. SIA for FortiClient agent remote users
C. Site-based remote user internet access
D. SIA using ZTNA

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
```

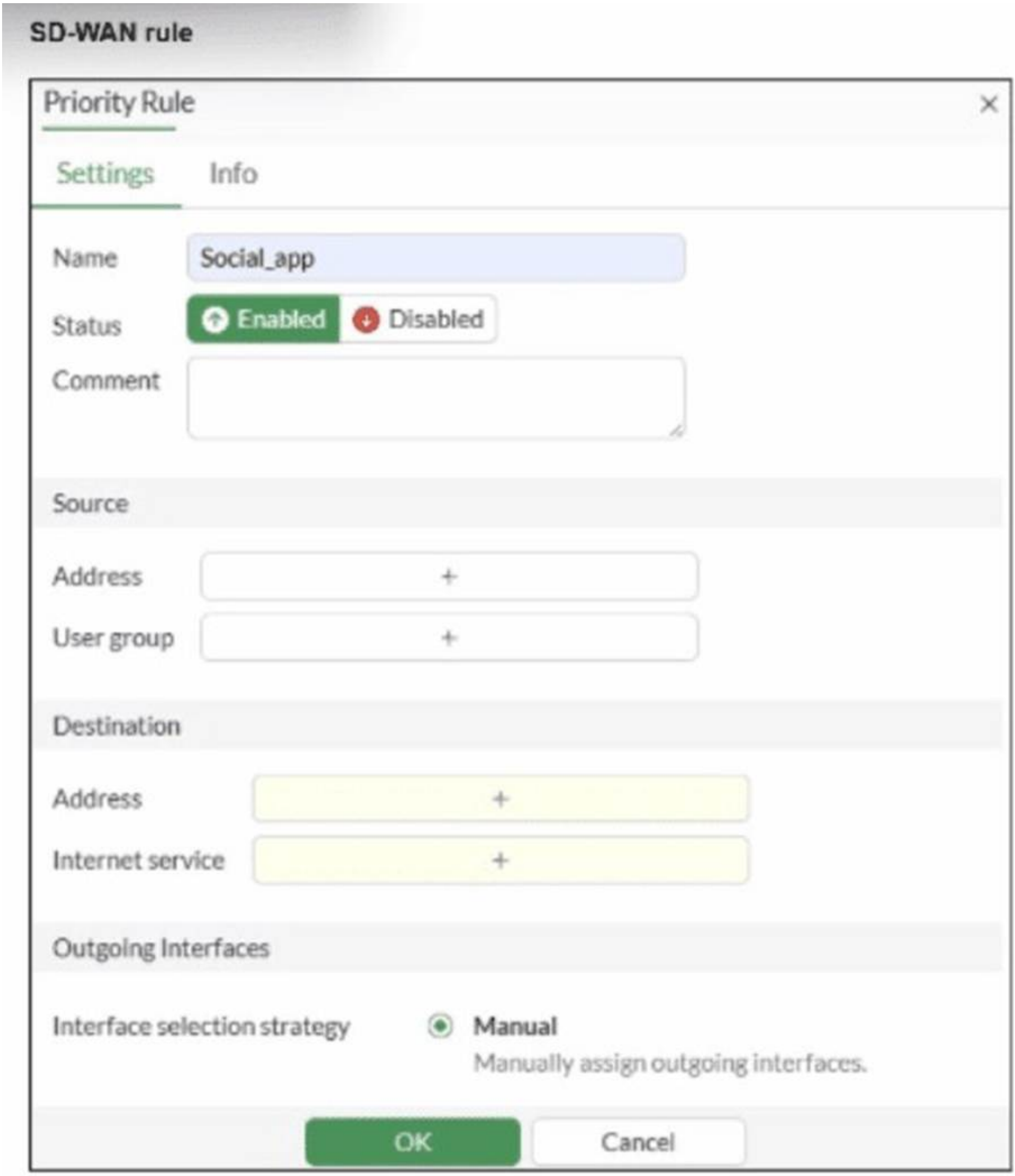
The exhibit shows output of the command diagnose sys sdwan service collected on a FortiGate device.
The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the social media application Facebook.
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.

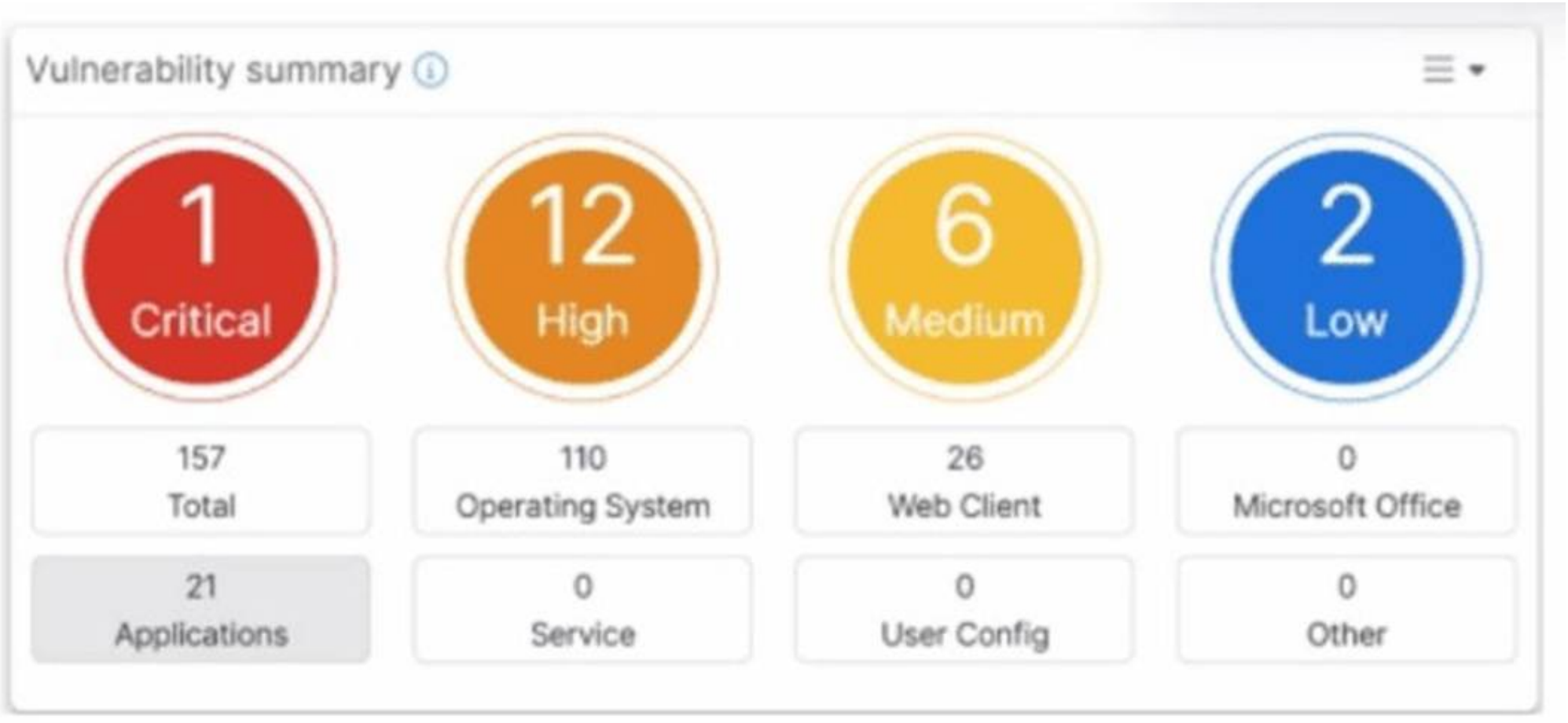


You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link. What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

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 7
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 8
An existing Fortinet SD-WAN customer who has recently deployed FortiSASE wants to have a comprehensive view of, and combined reports for, both SD-WAN branches and remote users. How can the customer achieve this?

A. Forward the logs from FortiSASE to Fortinet SOCaaS.
B. Forward the logs from FortiGate to FortiSASE.
C. Forward the logs from FortiSASE to the external FortiAnalyzer.
D. Forward the logs from the external SD-WAN FortiAnalyzer to FortiSASE.

Answer: C

NEW QUESTION 9
Which FortiSASE feature monitors SaaS application performance and connectivity to points of presence (POPs)?

A. Operations widgets
B. FortiView dashboards
C. Event logs
D. Digital experience monitoring

Answer: D

Explanation:
According to theFortiSASE 7.6 Administration GuideandDigital Experience Monitoring (DEM)documentation, the feature specifically designed to monitor SaaS application performance and connectivity to PoPs isDigital Experience Monitoring (DEM).
SaaS and Path Visibility: DEM assists administrators in troubleshooting remote user connectivity issues by providing enhanced health check visibility forSaaS applications, endpoint devices, and the network path. It provides real-time insights into application performance and latency issues.
PoP Connectivity: It monitors the digital journey from the end-user device through theSecurity Points of Presence (POPs)to the final application, identifying hops where degraded service (packet loss, delay, or jitter) is detected.
Proactive Management: By establishing thresholds and simulating user activities throughSynthetic Transaction Monitoring (STM), DEM allows IT teams to identify performance problems before they impact the business.
Why other options are incorrect:
Option A: Operations widgets provide general status overviews but do not offer the granular per-hop path analysis or specific SaaS transaction monitoring found in DEM.
Option B: FortiView dashboards provide traffic visibility and session data but are not dedicated performance monitoring tools for end-to-end digital experience.
Option C: Event logs record system occurrences and security events but do not provide real-time performance metrics or health check probes for SaaS

applications.

NEW QUESTION 10
Refer to the exhibit, which shows the SD-WAN rule status and configuration.

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority:2
      Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
      link-cost-factor(packet loss), link-cost-threshold(0), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), 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 (service) # show
config service
     edit 3
          set name "Corp"
          set mode priority
          set dst "Corp-net"
          set src "LAN-net"
          set health-check "HUB1_HC"
          set link-cost-factor packet-loss
          set link-cost-threshold 0
          set priority-members 6 4 5
     next
```

Based on the exhibit, which change in the measured packet loss will make HUB1-VPN3 the new preferred member? (Choose one answer)

A. When all three members have the same packet loss
B. When HUB1-VPN1 has 4% packet loss
C. When HUB1-VPN1 has 12% packet loss
D. When HUB1-VPN3 has 4% packet loss

Answer: A

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 12
Refer to the exhibits.

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]
```

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.)

A. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.
B. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
C. FortiGate routes only new sessions over port1.
D. FortiGate continues routing all existing sessions over port2.
E. FortiGate flags the sessions as dirty.

Answer: AE

NEW QUESTION 16
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 18
Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three answers)

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

Answer: BDE

NEW QUESTION 22
How does the FortiSASE security dashboard facilitate vulnerability management for FortiClient endpoints? (Choose one answer)

A. It automatically patches all vulnerabilities without user intervention and does not categorize vulnerabilities by severity.
B. It shows vulnerabilities only for applications and requires endpoint users to manually check for affected endpoints.
C. It displays only critical vulnerabilities, requires manual patching for all endpoints, anddoes not allow viewing of affected endpoints.
D. It provides a vulnerability summary, identifies affected endpoints, and supports automatic patching for eligible vulnerabilities.

Answer: D

Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administratortraining materials, the security dashboard is a centralized hub for monitoring and remediating security risks across the entire fleet of managed endpoints.
Vulnerability Summary: The dashboard includes a dedicatedVulnerability summary widgetthat categorizes risks by severity (Critical, High, Medium, Low) and by application type (OS, Web Client, etc.).
Identifying Affected Endpoints: The dashboard is fully interactive; an administrator candrill downinto specific vulnerability categories to view a detailed list ofCVE dataand, most importantly, identify the specificaffected endpointsthat require attention.
Automatic Patching: FortiSASE supportsautomatic patching for eligible vulnerabilities(such as common third-party applications and supported OS updates). This feature is configured within theEndpoint Profile, allowing the FortiClient agent to remediate risks without requiring the user to manually run updates.
Why other options are incorrect:
Option A: While it supports automatic patching, it does not do so forallvulnerabilities (only eligible/supported ones), and it specificallydoescategorize them by severity.
Option B: The dashboard shows vulnerabilities for theOperating Systemas well as applications, and it allows theadministratorto identify affected endpoints rather than requiring the end-user to check.
Option C: The dashboard displaysall levels of severity(not just critical) and explicitly allows the viewing of affected endpoints.

NEW QUESTION 23
Which statement is true about FortiSASE supported deployment?

A. FortiSASE supports VPN mode and Agentless mode, based on user requirements.
B. FortiSASE supports both Endpoint mode and SWG mode, depending on deployment.
C. FortiSASE operates only in SWG mode, where all traffic is forced through FortiSASE POPs.
D. FortiSASE relies on ZTNA-only mode, which replaces SWG and endpoint functions.

Answer: B

NEW QUESTION 25
.....

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