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
The IT team is wondering whether they will need to continue using MDM tools for future FortiClient upgrades.
What options are available for handling future FortiClient upgrades?

A. Enable the Endpoint Upgrade feature on the FortiSASE portal.
B. FortiClient will need to be manually upgraded.
C. Perform onboarding for managed endpoint users with a newer FortiClient version.
D. A newer FortiClient version will be auto-upgraded on demand.

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
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 6
What is the purpose of the on/off-net rule setting in FortiSASE?

A. To enable or disable user authentication for external network access.
B. To define different traffic routing rules for on-premises and cloud-based resources.
C. To determine if an endpoint is connecting from a trusted network or untrusted location.
D. To configure different access policies for users based on their geographical location.

Answer: C

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
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 9
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 10

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
Which configuration is a valid use case for FortiSASE features in supporting remote users?

A. Enabling secure SaaS access through SD-WAN integration, protecting against web- based threats with data loss prevention, and monitoring user connectivity with shadow IT visibility.
B. Monitoring SaaS application performance, isolating browser sessions for all websites, and integrating with SD-WAN for data loss prevention.
C. Enabling secure web browsing to protect against threats, providing explicit application access with zero-trust or SD-WAN integration, and addressing shadow IT visibility with data loss prevention.
D. Providing secure web browsing through remote browser isolation, addressing shadow IT with zero-trust access, and protecting data at rest only.

Answer: C

NEW QUESTION 13
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 16
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 21
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
DRAG DROP
In which order does a FortiGate device consider the following elements shown in the left column during the route lookup process?
Select the element in the left column, hold and drag it to a blank position in the column on the right. Place the four correct elements in order, placing the first element in the first position at the top of the column. Once you place an element, you can move it again if you want to change your answer before moving to the next question. You need to drop four elements in the work area.
Select and drag the screen divider to change the viewable area of the source and work areas.

Route Lookup Process

SD-WAN rules
Policy routes
Default routes
Internet Service Database (ISDB) routes
Connected routes

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 26
Refer to the exhibit.

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(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 96.349, selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 141.278, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 190.984, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (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 priority-members 4 5 6
    next
```

The SD-WAN rule status and configuration is shown. Based on the exhibit, which change in the measured latency will first make HUB1-VPN3 the new preferred member?

A. When HUB1-VPN3 has a latency of 80 ms
B. When HUB1-VPN3 has a lower latency than HUB1-VPN1 and HUB1-VPN2
C. When HUB1-VPN1 has a latency of 200 ms
D. When HUB1-VPN3 has a latency of 90 ms

Answer: A

NEW QUESTION 29
.....

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