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


```
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
```

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
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 12
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 15
.....

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