# Download Fortinet NSE5_SSE_AD-7.6 Exam Dumps Free

**Shared by Willis on 17-06-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

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

## Options:

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

## Explanation:

According to the FortiSASE 7.6 Architecture Guide and Administration Guide, the Site-based remote user internet access use case is the only deployment model that completely eliminates the need for individual endpoint configuration.

Centralized Enforcement: In a site-based deployment, a 'thin edge' device (such as a FortiExtender or a FortiGate in LAN extension mode) is installed at the remote site. This device establishes a secure tunnel to the FortiSASE Point of Presence (PoP).

Zero Endpoint Configuration: Because the traffic redirection happens at the network gateway level, individual devices (laptops, IoT devices, mobile phones) behind the site-based device do not require any specialized software or settings. They simply connect to the local network as they would normally, and their traffic is automatically secured by the SASE cloud.

Comparison with Other Modes:

Agent-based (Option B): Requires the installation and maintenance of FortiClient software on every device, often managed via MDM tools.

Agentless (Option A): While it doesn't need an agent, it typically requires the configuration of Explicit Web Proxy settings or the distribution of a PAC (Proxy Auto-Configuration) file via GPO or SCCM to each device's browser.

ZTNA (Option D): Generally requires an endpoint agent (FortiClient) to perform posture checks and identity verification, involving significant endpoint-level configuration.

Why other options are incorrect:

Option A: Agentless mode is often confused with being 'configuration-free,' but it still requires endpoints to be pointed toward the FortiSASE proxy.

Option B: This is the most configuration-intensive mode, requiring full software lifecycles for every endpoint.

Option D: ZTNA is an access methodology that adds configuration complexity (tags, certificates, posture checks) rather than minimizing it.

# Question 2

Question Type: MultipleChoice

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? (Select two.)

## Options:

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:

A, C

## Explanation:

According to the SD-WAN 7.6 Core Administrator curriculum and the diagnostic outputs shown in the exhibit, the reason traffic is steered to HUB1-VPN3 instead of the expected HUB1-VPN1 (defined in SD-WAN rule ID 1) can be explained by two core routing principles in FortiOS:

Valid Route Requirement (Option A): In the diagnose sys sdwan service 4 output (which corresponds to Rule ID 1), it shows the rule has members HUB1-VPN1, HUB1-VPN2, and HUB1-VPN3. A key principle of SD-WAN steering is that for a member to be 'selectable' by a rule, it

must have a valid route to the destination in the routing table (RIB/FIB). If the routing table output (the third section of the exhibit) shows a route to 10.0.0.0/8 via HUB1-VPN3 but not through HUB1-VPN1, the SD-WAN engine will skip HUB1-VPN1 entirely because it is considered a 'non-reachable' path for that specific destination.

Policy Route Precedence (Option D): In the FortiOS route lookup hierarchy, Regular Policy Routes (PBR) are evaluated before SD-WAN rules. If an administrator has configured a traditional Policy Route (found under Network > Policy Routes) that matches traffic destined for 10.0.0.0/8 and specifies HUB1-VPN3 as the outgoing interface, the FortiGate will forward the packet based on that policy route and will never evaluate the SD-WAN rules for that session. This 'bypass' occurs regardless of whether the SD-WAN rule would have chosen a 'better' link.

Why other options are incorrect:

Option B: While member configuration priority (cfg_order) is a tie-breaker in some strategies, the SD-WAN rule logic is only applied if the routing table allows it or if a higher-priority policy route doesn't intercept the traffic first.

Option C: Lower route priority (which means higher preference in the RIB) affects the Implicit Rule (standard routing). However, SD-WAN rules are designed to override RIB priority for matching traffic. If HUB1-VPN1 was a valid candidate and no Policy Route existed, the SD-WAN rule would typically ignore RIB priority to enforce its own steering strategy.

# Question 3

Question Type: MultipleChoice

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

## Options:

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, and does 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 the FortiSASE 7.6 Administration Guide and the FCP - FortiSASE 24/25 Administrator training 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 dedicated Vulnerability summary widget that 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 can drill down into specific vulnerability categories to view a detailed list of CVE data and, most importantly, identify the specific affected endpoints that require attention.

Automatic Patching: FortiSASE supports automatic patching for eligible vulnerabilities (such as common third-party applications and supported OS updates). This feature is configured within the Endpoint 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 for all vulnerabilities (only eligible/supported ones), and it specifically does categorize them by severity.

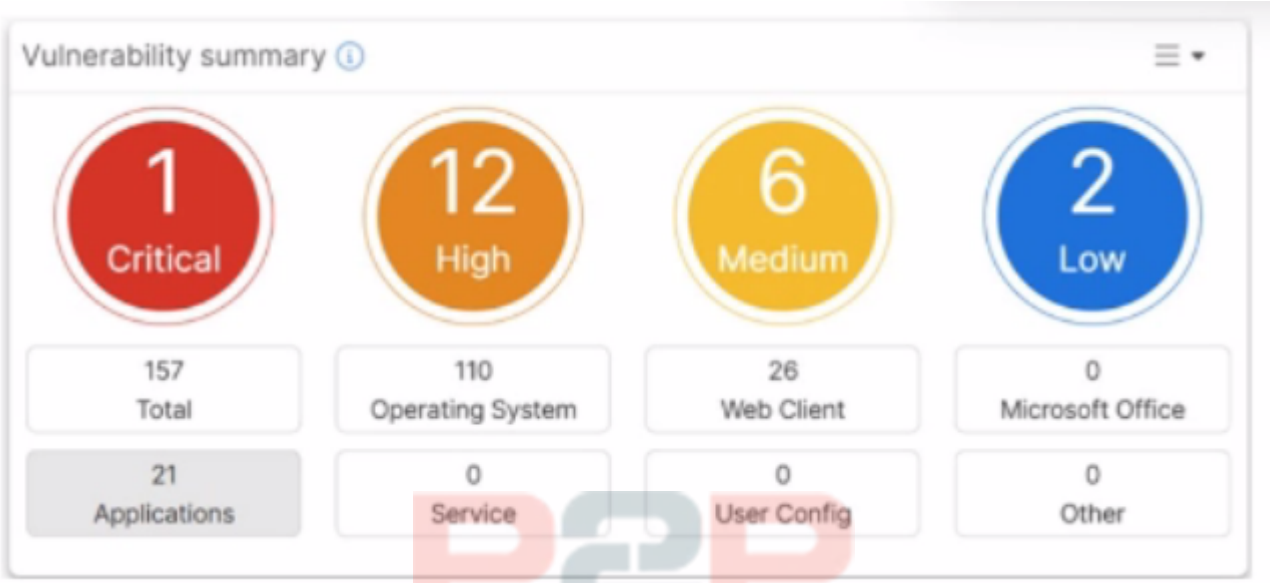
Option B: The dashboard shows vulnerabilities for the Operating System as well as applications, and it allows the administrator to identify affected endpoints rather than requiring the end-user to check.

Option C: The dashboard displays all levels of severity (not just critical) and explicitly allows the viewing of affected endpoints.

# Question 4

Question Type: MultipleChoice

Refer to the exhibit.




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

## Options:

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:

C, D

## Explanation:

Based on the FortiSASE 7.6 (and later 2025 versions) curriculum and administration guides, the Vulnerability summary dashboard is a key component of the endpoint security posture management.

Drill Down Capability (Option C): According to the FortiSASE Administration Guide, the Vulnerability summary widget on the Security dashboard is interactive. An administrator can click on specific risk categories (e.g., Critical, High) or application types (e.g., Operating System, Web Client) to drill down. This action opens a detailed pane showing the specific affected endpoints, associated CVE identifiers, and severity classifications based on the CVSS standard.

Automatic Vulnerability Patching (Option D): In the FortiSASE 7.6/2025 feature sets, the endpoint profile configuration (under Endpoint > Configuration > Profiles) includes an 'Automatic Patching' section. This feature allows the system to automatically install security updates for supported

third-party applications and the underlying operating system (Windows/macOS) when vulnerabilities are detected. Furthermore, administrators can schedule these patches directly from the Vulnerability Summary widget by selecting specific vulnerabilities.

Why other options are incorrect:

Option A: The dashboard categories (Operating System, Web Client, Microsoft Office, etc.) are based on known software signatures. While there is an 'Other' category, the dashboard primarily provides scores for recognized applications where CVE data is available.

Option B: The exhibit shows active data (157 total vulnerabilities), which indicates that the vulnerability scan is enabled and currently reporting data from the endpoints. If it were disabled, the widget would be empty or show zeros.



# Question 5

Question Type: MultipleChoice

Which statement is true about FortiSASE supported deployment?

## Options:

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

## Explanation:

According to the FortiSASE 7.6 Administration Guide and the FCP - FortiSASE 24/25 Administrator curriculum, FortiSASE is designed with a hybrid deployment architecture to support various user and device requirements. It primarily operates in two modes:

Endpoint Mode (Agent-based): This mode requires the installation of FortiClient on the user's laptop or device. The agent establishes an 'always-up' secure VPN tunnel to the nearest FortiSASE Point of Presence (PoP), providing full Secure Internet Access (SIA), Secure Private Access (SPA), and endpoint posture checks (ZTNA).

Secure Web Gateway (SWG) Mode (Agentless): This mode is used for users or devices where installing an agent is not feasible (e.g., unmanaged devices or Chromebooks). It relies on explicit web proxy settings or a PAC (Proxy Auto-Configuration) file to redirect web traffic (HTTP/HTTPS) to the SASE PoP for inspection.

Why other options are incorrect:

Option A: While it supports VPN, 'VPN mode' is not the formal name of the deployment type; it is 'Endpoint mode'.

Option C: FortiSASE is not limited to SWG; it is a full SSE (Security Service Edge) solution including FWaaS and ZTNA.

Option D: ZTNA is a capability within the platform, not a replacement for the overall endpoint or SWG functions.

# Question 6

Question Type: MultipleChoice

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

## Options:

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:

B, D, E

## Explanation:

According to the SD-WAN 7.6 Core Administrator study guide and the Fortinet Document Library,

the interaction between SD-WAN rules and SLA targets is governed by specific selection and measurement logic:

Usage by Strategy (Option B): SLA targets are fundamentally used by the Lowest Cost (SLA) strategy to determine which links are currently healthy enough to be considered for traffic steering. While other strategies like Best Quality use a 'Measured SLA' to monitor metrics, they do not typically use the 'Required SLA Target' to disqualify links unless specifically configured in a hybrid mode. In most curriculum contexts, the 'Required SLA Target' field is specifically associated with the Lowest Cost and Maximize Bandwidth strategies.

SLA Compliance Checking (Option D): SD-WAN rules utilize SLA targets as a 'pass/fail' gatekeeper. The engine checks if the preferred members meet the defined SLA requirements (latency, jitter, or packet loss thresholds). If a preferred member fails the SLA, the rule will move to the next member in the priority list that does meet the SLA.

Single SLA Binding (Option E): When configuring an SD-WAN rule, the GUI and CLI allow you to select multiple SLA targets, but they must all belong to the same Performance SLA profile. You cannot mix and match targets from different health checks (e.g., Target 1 from 'Google_HC' and Target 2 from 'Amazon_HC') within a single SD-WAN rule.

Why other options are incorrect:

Option A: This is incorrect because a single SD-WAN rule can only be associated with one specific Performance SLA profile at a time; therefore, you cannot select targets from different SLAs.

Option C: This is incorrect because member metrics (latency, jitter, packet loss) are measured by the Performance SLA probes regardless of whether an SD-WAN rule is currently using that SLA target for steering decisions. Measurement is a function of the health-check, not the rule matching process.