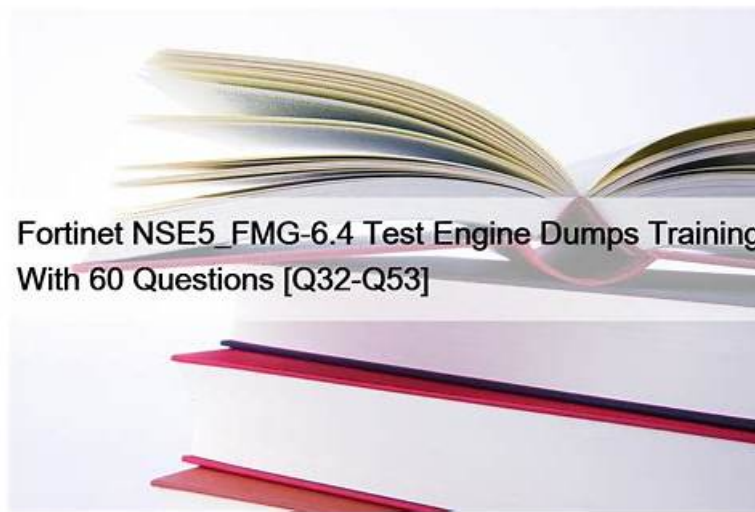


# 100% Pass-Rate Reliable NSE5\_SSE\_AD-7.6 Test Braindumps–The Best Brain Exam for NSE5\_SSE\_AD- 7.6 - Perfect Braindumps NSE5\_SSE\_AD-7.6 Torrent



Lead2Passed provides updated and valid Fortinet NSE5\_SSE\_AD-7.6 Exam Questions because we are aware of the absolute importance of updates, keeping in mind the dynamic Fortinet NSE5\_SSE\_AD-7.6 Exam Syllabus. We provide you update checks for 365 days after purchase for absolutely no cost.

## Fortinet NSE5\_SSE\_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Secure Internet Access (SIA) and Secure SaaS Access (SSA): This section focuses on implementing security profiles for content inspection and deploying compliance rules to managed endpoints.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.</li></ul>
Topic 5	<ul style="list-style-type: none"><li>Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.</li></ul>

>> Reliable NSE5\_SSE\_AD-7.6 Test Braindumps <<

## Most Trusted Platform to Buy Fortinet NSE5\_SSE\_AD-7.6 Actual Dumps

There are some education platforms in the market for college students or just for the use of office workers, which limits the user groups of our NSE5\_SSE\_AD-7.6 study guide to a certain extent. And we have the difference compared with the other NSE5\_SSE\_AD-7.6 Quiz materials for our study materials have different learning segments for different audiences. We have three different versions of our NSE5\_SSE\_AD-7.6 exam questions on the formats: the PDF, the Software and the APP online.

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

## Questions (Q24-Q29):

### NEW QUESTION # 24

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

**Answer: C,D,E**

Explanation:

**Routing:** For a packet to even be considered by the SD-WAN engine, there must be a matching route in the Forwarding 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 the SD-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.

**Interfaces:** You must first define the physical or logical interfaces (such as ISP links, LTE, or VPN tunnels) as SD-WAN members. These members are then typically grouped into SD-WAN Zones.

Without designated member interfaces, there is no "pool" of links for the SD-WAN rules to select from.

**Firewall Policies:** In FortiOS, no traffic is allowed to pass through the device unless a Firewall Policy permits it. To steer traffic, you must have a policy where the Incoming Interface is the internal network and the Outgoing Interface is 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.

### NEW QUESTION # 25

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

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

**Answer: B,C**

Explanation:

According to the SD-WAN 7.6 Core Administrator study guide and the FortiOS 7.6 Administration Guide, configuring load balancing within SD-WAN rules requires an understanding of how the engine selects and distributes sessions across multiple links.

\* SLA Target Logic (Option A): In FortiOS 7.6, the Lowest Cost (SLA) strategy has been enhanced.

When the load-balance option is enabled for this strategy, the FortiGate does not just pick a single "best" link; it identifies all member interfaces that currently meet the configured SLA target (e.g., latency < 100ms). It then load balances the traffic across all those healthy links to maximize resource utilization.

\* Hash Modes (Option D): When an SD-WAN rule is configured for load balancing (valid for Manual and Lowest Cost (SLA) strategies in 7.6), the administrator must define a hash mode to determine how sessions are distributed. While "outsessions" in the question is a common exam-variant typo for outbandwidth (or sessions-based hashing), the core principle remains: you can select the specific load-balancing algorithm (e.g., source-ip, round-robin, or bandwidth-based) for all strategies where load-balancing is enabled.

Why other options are incorrect:

\* Option B and C: These options are too restrictive. In FortiOS 7.6, load balancing is not limited to only "manual and best quality" or "manual and lowest cost" in a singular way. The documentation highlights that Manual and Lowest Cost (SLA) are the primary strategies that support the explicit load-balance toggle to steer traffic through multiple healthy members simultaneously.

### NEW QUESTION # 26

How does the FortiSASE security dashboard facilitate vulnerability management for FortiClient endpoints?

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

**Answer: C**

Explanation:

The FortiSASE security dashboard presents a full vulnerability summary, shows which endpoints are affected, and supports automatic patching for vulnerabilities that are eligible for automated remediation.

#### NEW QUESTION # 27

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

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

**Answer: A,C,D**

#### NEW QUESTION # 28

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

- A. Providing secure web browsing through remote browser isolation, addressing shadow IT with zero-trust access, and protecting data at rest only.
- **B. 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.**
- C. 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.
- D. Monitoring SaaS application performance, isolating browser sessions for all websites, and integrating with SD-WAN for data loss prevention.

**Answer: B**

Explanation:

According to the FortiSASE 7.6 Architecture Guide and FCP - FortiSASE 24/25 Administrator materials, the solution is built around three primary use cases that support a hybrid workforce:

\* Secure Internet Access (SIA): This enables secure web browsing by applying security profiles such as Web Filter, Anti-Malware, and SSL Inspection in the SASE cloud. It protects remote users from internet-based threats regardless of their location.

\* Secure Private Access (SPA): This provides granular, explicit access to private applications hosted in data centers or the cloud. It is achieved through ZTNA (Zero Trust Network Access) for session-based security or through SD-WAN integration where FortiSASE acts as a spoke to an existing corporate SD-WAN hub.

\* SaaS Security: FortiSASE utilizes Inline-CASB and Shadow IT visibility to monitor and control the use of cloud applications. Data Loss Prevention (DLP) is integrated into these workflows to prevent sensitive corporate data from being uploaded to unauthorized SaaS platforms.

Why other options are incorrect:

\* Option A: While it mentions SD-WAN and Shadow IT, it misses the core definition of SIA (secure web browsing) which is the primary driver for SASE deployments.

\* Option B: Remote Browser Isolation (RBI) is typically applied to risky or uncategorized websites, not "all websites," due to the high performance and resource overhead.

\* Option D: FortiSASE is designed to protect data in motion (via security profiles) as well as data stored in sanctioned cloud apps, not "at rest only".

• • • • •

**Brain NSE5\_SSE\_AD-7.6 Exam:** [https://www.lead2passed.com/Fortinet/NSE5\\_SSE\\_AD-7.6-practice-exam-dumps.html](https://www.lead2passed.com/Fortinet/NSE5_SSE_AD-7.6-practice-exam-dumps.html)

- [illegible]