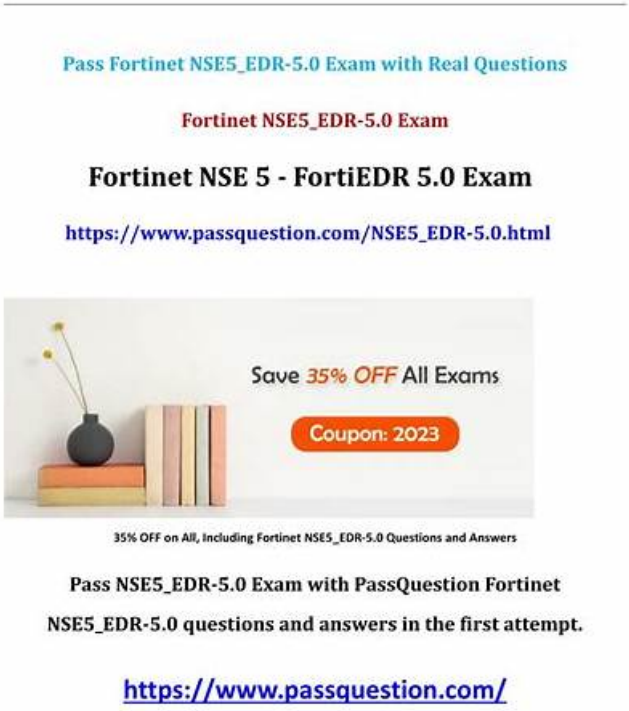
Fortinet NSE5_SSE_AD-7.6 Reliable Exam Test - NSE5_SSE_AD-7.6 Practice Test Pdf



Prep4King is a rich-experienced website specialized in the Fortinet dump torrent and real pdf dumps. These pdf study materials are concluded by our professional IT trainers who have a good knowledge of NSE5_SSE_AD-7.6 Exam Questions torrent. They check the updating of vce braindumps every day to ensure the accuracy of NSE5_SSE_AD-7.6 test questions and answers.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 3	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.
Topic 4	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.

Topic 5	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.

NSE5_SSE_AD-7.6 Practice Test Pdf - NSE5_SSE_AD-7.6 Practice Exam Pdf

It is a prevailing belief for many people that practice separated from theories are blindfold. Our NSE5_SSE_AD-7.6 learning quiz is a salutary guidance helping you achieve success. The numerous feedbacks from our clients praised and tested our strength on this career, thus our NSE5_SSE_AD-7.6 practice materials get the epithet of high quality and accuracy.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q30-Q35):

NEW QUESTION # 30
Which statement about security posture tags in FortiSASE is correct?

- A. Multiple tags can be assigned to an endpoint and used for evaluation.
- B. Tags are static and do not change with endpoint status.
- C. Only one tag can be assigned to an endpoint.
- D. Multiple tags can be assigned to an endpoint, but only one is used for evaluation.

Answer: A

Explanation:
According to theFortiSASE 7.6 Administration GuideandFCP - FortiSASE 24/25 Administrator curriculum, security posture tags (often referred to as ZTNA tags) are the fundamental building blocks for identity-based and posture-based access control.
* Multiple Tag Assignment: A single endpoint can be assigned multiple tags at the same time. For example, an endpoint might simultaneously have the tags"OS-Windows-11","AV-Running", and
"Corporate-Domain-Joined".
* Evaluation Logic: During the policy evaluation process (for both SIA and SPA), FortiSASE or the FortiGate hub considers all tags assigned to the endpoint. Security policies can be configured to use these tags as source criteria. If an administrator defines a policy that requires both "AV-Running" and
"Corporate-Domain-Joined," the system evaluates both tags to decide whether to permit the traffic.
* Dynamic Nature: Contrary to Option C, these tags are highly dynamic. They are automatically applied or removed in real-time based on the telemetry data sent by theFortiClientto the SASE cloud. If a user disables their antivirus, the "AV-Running" tag is removed immediately, and the endpoint's access is revoked by the next policy evaluation.
* Scalability: While the system supports many tags, documentation recommends a baseline of custom tags for optimal performance, though it confirms that multiple tags are standard for reflecting a comprehensive security posture.
Why other options are incorrect:
* Option A: This is incorrect because the system does not pick just one tag; it evaluates the collection of tags against the policy's requirements (e.g., matching any or matching all).
* Option C: This is incorrect because tags are dynamic and change as soon as the endpoint's status (like vulnerability count or software presence) changes.
* Option D: This is incorrect because the architectural advantage of ZTNA is the ability to layer multiple security "checks" (tags) for a single user.

NEW QUESTION # 31
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.)

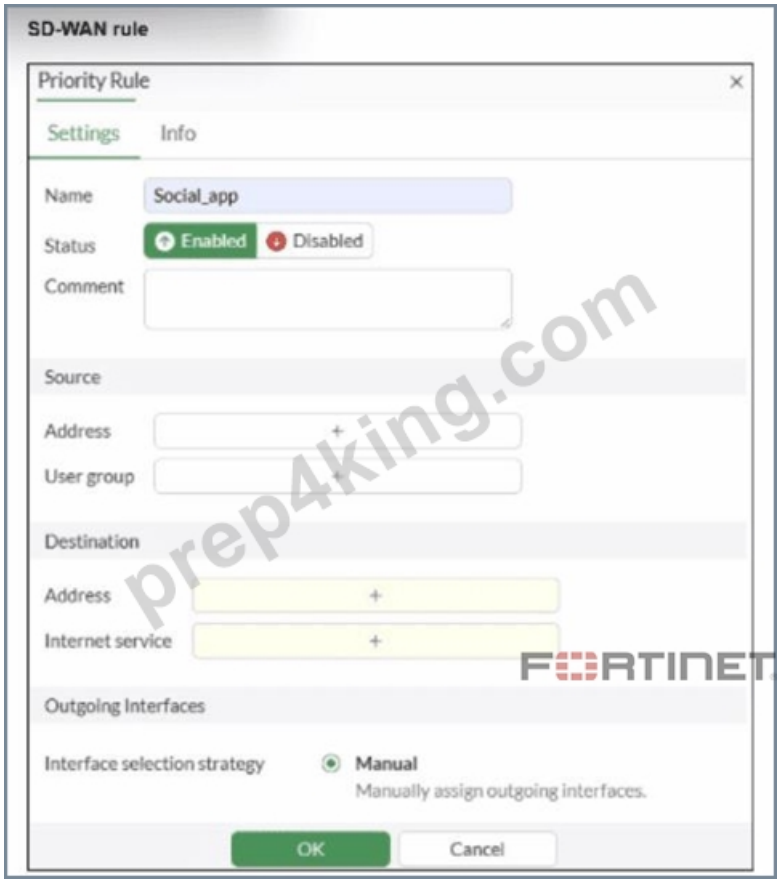
- A. Interfaces
- B. Firewall policies
- C. Traffic shaping
- D. Security profiles

- E. Routing

Answer: A,B,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 # 32
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. In the Internet service field, select Facebook and LinkedIn.
- B. Install a license to allow applications as destinations of SD-WAN rules.
- 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: A

Explanation:
According to theSD-WAN 7.6 Core Administratorcurriculum and theFortiOS 7.6 Administration Guide, setting common web-based services like Facebook and LinkedIn as destinations in an SD-WAN rule is primarily accomplished through theInternet

Service Database (ISDB).
* Internet Service vs. Application Control: In FortiOS, there is a distinction betweenInternet Services (which use a database of known IP addresses and ports to identify traffic at the first packet) and Applications(which require the IPS engine to inspect deeper into the packet flow to identify Layer 7 signatures).
* SD-WAN Efficiency: Fortinet recommends using theInternet service fieldfor services like Facebook and LinkedIn in SD-WAN rules because it allows the FortiGate to steer the traffic immediately upon the first packet. If the "Application" signatures were used instead, the first session might be misrouted because the application is not identified until after the initial handshake.
* GUI Configuration: As shown in the exhibit (image_b3a4c2.png), the "Destination" section of an SD- WAN rule includes anInternet servicefield by default. To steer Facebook and LinkedIn traffic, the administrator simply clicks the "+" icon in that field and selects the entries for Facebook and LinkedIn from the database.
* Feature Visibility (Alternative): While youcanenable a specific "Application" field inSystem > Feature Visibility(by enabling "Application Detection Based SD-WAN"), this is typically used for less common applications that do not have dedicated ISDB entries. For the specific "applications" mentioned (Facebook and LinkedIn), they are natively available in theInternet servicefield, making Option B the most direct and common implementation.
Why other options are incorrect:
* Option A: Licensing for application signatures is part of the standard FortiGuard services and is not a prerequisite specific only to "applications as destinations" in SD-WAN rules.
* Option C: Standalone FortiGate devices fully support application-based and ISDB-based steering in SD-WAN rules.
* Option D: While enabling feature visibility would add anadditionalfield for L7 applications, it is not a "must" for Facebook and LinkedIn, which are already accessible via the Internet Service field provided in the default GUI layout.

NEW QUESTION # 33
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. Remove the member from the performance service-level agreement (SLA) definitions.
- C. Delete static route definitions for that interface.
- D. Disable the interface.

Answer: B

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortinet Document Library, FortiOS maintains strict referential integrity for SD-WAN objects. An SD-WAN member interface cannot be deleted or removed from the configuration if it is still being "used" or referenced by other features.
* Reference Locking: In the FortiOS GUI, the "Delete" button for an SD-WAN member is typically grayed out or an error message appears if the interface is part of an active service or monitoring tool.
* Performance SLA Dependency: Performance SLAs (health checks) monitor specific member interfaces. If an interface is a participant in an SLA, it is considered "active" by the system. Therefore, a critical first step in the decommissioning process is toremove the member from all Performance SLA definitions. Once the health check is no longer polling that interface, one major reference lock is released.
* Other Dependencies: While firewall policies and SD-WAN rules (service rules) also create references, the question specifies the member is "no longer used to steer traffic," implying it may have already been removed from steering rules. However, Performance SLAs often remain active in the background, making their removal the essential next step to permit the deletion of the member itself.
Why other options are incorrect:
* Option A: Moving a member between zones doesn't help you delete it; it just changes its logical grouping. It still remains an active SD-WAN member.
* Option B: Disabling the physical interface does not remove the configuration references within the SD- WAN engine. The FortiGate will simply report the member as "Down," but it will still exist in the configuration as a member.
* Option D: In modern SD-WAN deployments, static routes usually point to theSD-WAN Zone(like virtual-wan-link) rather than individual physical interfaces. Therefore, you don't typically need to delete the static route to remove a single member from the zone.

NEW QUESTION # 34
You have configured the performance SLA with the probe mode as Prefer Passive.
What are two observable impacts of this configuration? (Choose two.)

- A. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.
- B. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
- C. FortiGate passively monitors the member if ICMP traffic is passing through the member.
- D. FortiGate passively monitors the member if TCP traffic is passing through the member.
- E. During passive monitoring, the SLA performance rule cannot detect dead members.

Answer: D,E

Explanation:
When "Prefer Passive" is set, FortiGate attempts to passively monitor the health of SD-WAN members using real application traffic like TCP sessions, collecting statistics such as latency, jitter, and packet loss from actual observed flows.
Passive monitoring does not generate probe packets; it relies entirely on existing traffic. If there is no matching traffic, health check data is unavailable, meaning dead members may go undetected when only passive monitoring is active.

NEW QUESTION # 35
......

Prep4King team of professionals made this product after working day and night so that users can prepare from it for the Fortinet NSE5_SSE_AD-7.6 certification test successfully. Prep4King even guarantees that you will pass the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) test on the first try by preparing with real questions. If you fail to pass the certification exam, despite all your efforts, you could get a full refund from Prep4King according to terms and conditions.

NSE5_SSE_AD-7.6 Practice Test Pdf: https://www.prep4king.com/NSE5_SSE_AD-7.6-exam-prep-material.html

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes