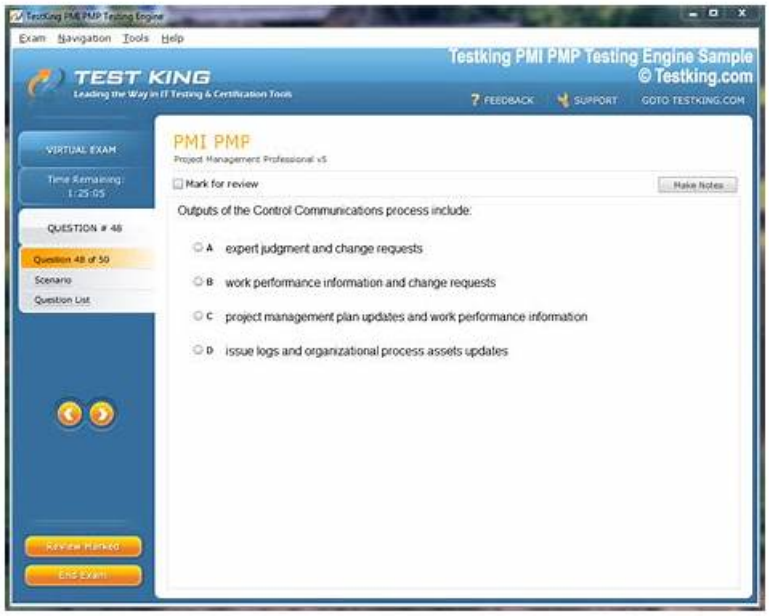
NSE5_SSE_AD-7.6 Valid Exam Testking & Reliable NSE5_SSE_AD-7.6 Dumps Sheet



We offer you NSE5_SSE_AD-7.6 study guide with questions and answers, and you can practice it by concealing the answers, and when you have finished practicing, you can cancel the concealment, through the way like this, you can know the deficient knowledge for NSE5_SSE_AD-7.6 exam dumps, so that you can put your attention to the disadvantages. In addition, we also have the free demo for NSE5_SSE_AD-7.6 Study Guide for you to have a try in our website. These free demos will give you a reference of showing the mode of the complete version. If you want NSE5_SSE_AD-7.6 exam dumps, just add them into your card.

We have first-rate information protection system, if you purchasing NSE5_SSE_AD-7.6 exam materials from us, we can ensure you that the safety of your email box. We respect your privacy and will never send junk email to you. NSE5_SSE_AD-7.6 exam dumps of us are also high-quality, and will help you pass the exam and get the certificate successfully. What's more, we have professional online chat service stuff, if you have any questions about the NSE5_SSE_AD-7.6 Exam Materials, just have a conversation with them. We will give you reply as quickly as possible.

>> NSE5_SSE_AD-7.6 Valid Exam Testking <<

Fortinet NSE5_SSE_AD-7.6 Latest Dumps - Affordable Price and Free Updates

Just choose the right PDFVCE Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Questions formats and download quickly and start NSE5_SSE_AD-7.6 exam preparation without wasting further time. The countless NSE5_SSE_AD-7.6 exam candidates have already passed their dream Fortinet NSE5_SSE_AD-7.6 Certification Exam and they all have got help from PDFVCE NSE5_SSE_AD-7.6 exam questions. You can also trust PDFVCE NSE5_SSE_AD-7.6 exam practice test questions and start preparation right now.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 2	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.

Topic 3	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.
Topic 4	• 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 5	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q32-Q37):

NEW QUESTION # 32
Which secure internet access (SIA) use case minimizes individual endpoint configuration? (Choose one answer)

- A. SIA for FortiClient agent remote users
- B. Agentless remote user internet access
- C. SIA using ZTNA
- D. Site-based remote user internet access

Answer: D

Explanation:
According to theFortiSASE 7.6 Architecture GuideandAdministration Guide, theSite-based remote user internet accessuse 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 aFortiExtender or aFortiGatein 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 ofFortiClientsoftware 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 Proxysettings or the distribution of aPAC (Proxy Auto-Configuration) filevia 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.

NEW QUESTION # 33
A FortiGate device is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN. What must you do as part of this configuration update process? (Choose one answer)

- A. Disable the interface that you want to use as an SD-WAN member.
- B. Replace references to interfaces used as SD-WAN members in the routing configuration.
- C. Purchase and install the SD-WAN license, and reboot the FortiGate device.
- D. Replace references to interfaces used as SD-WAN members in the firewall policies.

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, when you are migrating a production FortiGate to use SD-WAN, the most critical step involves reconfiguring how traffic is permitted and routed.

* Reference Removal Requirement: Before an interface (such as wan1 or wan2) can be added as anSD- WAN member, it must be "unreferenced" in most parts of the FortiGate configuration. Specifically, if an interface is currently being used in an activeFirewall Policy, the system will prevent you from adding it to the SD-WAN bundle.
* Firewall Policy Migration (Option A): In a production environment, you mustreplace the references to the physical interfacesin your firewall policies with the newSD-WAN virtual interface(or an SD- WAN Zone). For example, if your previous policy allowed traffic from internal to wan1, you must update that policy so theOutgoing Interfaceis now SD-WAN. This allows the SD-WAN engine to take over the traffic and apply its steering rules.
* Modern Tools: While this used to be a purely manual process, FortiOS 7.x includes anInterface Migration Wizard(found underNetwork > Interfaces). This tool automates the "search and replace" function, moving all existing policy and routing references from the physical port to the SD-WAN object to ensure minimal downtime.
Why other options are incorrect:
* Option B: While you do need to update your routing (e.g., creating a static route for 0.0.0.0/0 pointing to the SD-WAN interface), the curriculum specifically emphasizes the replacement of references in firewall policiesas the primary administrative hurdle, as policies are often more numerous and complex than the single static route required for SD-WAN.
* Option C: You donotneed to disable the interface. It must be up and configured, just removed from other configuration references so it can be "absorbed" into the SD-WAN bundle.
* Option D: SD-WAN is abase featureof FortiOS and doesnot require a separate licenseor a reboot to enable.

NEW QUESTION # 34
Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three answers)

- A. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.
- B. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.
- C. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.
- D. Member metrics are measured only if a rule uses the SLA target.
- E. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

Answer: A,B,E

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortinet 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 theLowest Cost (SLA)strategy to determine which links are currently healthy enough to be considered for traffic steering. While other strategies likeBest Qualityuse 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 thepreferred membersmeet 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 selectmultiple SLA targets, but they must all belong to thesame Performance SLAprofile. 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 fromdifferentSLAs.
* Option C: This is incorrect because member metrics (latency, jitter, packet loss) are measured by the Performance SLAprobes 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.

NEW QUESTION # 35
How is the Geofencing feature used in FortiSASE? (Choose one answer)

- A. To encrypt data at rest on mobile devices in specific countries.
- B. To restrict access to applications based on the time of day in specific countries.
- C. To allow or block remote user connections to FortiSASE POPs from specific countries.
- D. To monitor user behavior on websites and block non-work-related content from specific countries

Answer: C

Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administratorstudy materials, theGeofencingfeature is a security measure implemented at the edge of the FortiSASE cloud to control ingress connectivity based on the physical location of the user.
* Access Control by Location (Option A): Geofencing allows administrators toallow or block remote user connectionsto the FortiSASE Points of Presence (PoPs) based on the source country, region, or specific network infrastructure (e.g., AWS, Azure, GCP).
* Scope of Application: This feature is universal across all SASE connectivity methods. It applies to Agent-based users(FortiClient),Agentless users(SWG/PAC file), andEdge devices(FortiExtender /FortiAP). If a user attempts to connect from a blacklisted country, the connection is dropped at the PoP level before the user can even attempt to authenticate.
* Use Case Example: An organization operating exclusively in North America might configure geofencing toblock all connections originating from outside the US and Canada. This significantly reduces the attack surface by preventing brute-force or unauthorized access attempts from high-risk regions or countries where the organization has no legitimate employees.
* Configuration Path: In the FortiSASE portal, this is managed underConfiguration > Geofencing.
From there, administrators can create an "Allow" or "Deny" list and select the relevant countries from a standardized global database.
Why other options are incorrect:
* Option B: While FortiSASE supportsTime-based schedulesfor firewall policies, geofencing is specifically an IP-to-Geography mapping tool for connection admission, not a time-of-day restriction tool.
* Option C: Encryption of data at rest on mobile devices is a function of anMDM (Mobile Device Management)solution or local OS features (like FileVault or BitLocker), not a SASE network geofencing feature.
* Option D: Monitoring web behavior and blocking non-work content is the role of theWeb Filterand Application Controlprofiles, which operate on the trafficafterthe connection is allowed by geofencing.

NEW QUESTION # 36
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. Remove the member from the performance service-level agreement (SLA) definitions.
- B. Move the SD-WAN member to the virtual-wan-link zone.
- C. Delete static route definitions for that interface.
- D. Disable the interface.

Answer: A

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 # 37

......

Here in this Desktop practice test software, the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) practice questions given are very relevant to the actual Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam. It is compatible with Windows computers. PDFVCE provides its valued customers with customizable Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) practice exam sessions. The Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) practice test software also keeps track of the previous Fortinet NSE5_SSE_AD-7.6 practice exam attempts.

Reliable NSE5_SSE_AD-7.6 Dumps Sheet: https://www.pdfvce.com/Fortinet/NSE5_SSE_AD-7.6-exam-pdf-dumps.html