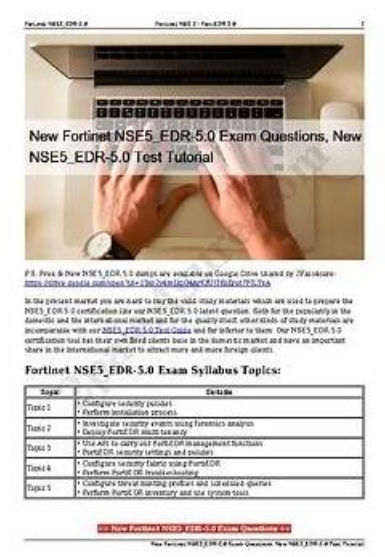
New NSE5_SSE_AD-7.6 Test Sims - Valid Test NSE5_SSE_AD-7.6 Vce Free



Are you worried about you poor life now and again? Are you desired to gain a decent job in the near future? Do you dream of a better life? Do you want to own better treatment in the field? If your answer is yes, please prepare for the NSE5_SSE_AD-7.6 exam. It is known to us that preparing for the exam carefully and getting the related certification are very important for all people to achieve their dreams in the near future. It is a generally accepted fact that the NSE5_SSE_AD-7.6 Exam has attracted more and more attention and become widely acceptable in the past years.

Our website PDFDumps provide the NSE5_SSE_AD-7.6 test guide to clients and help they pass the test NSE5_SSE_AD-7.6 certification which is highly authorized and valuable. Our company is a famous company which bears the world-wide influences and our NSE5_SSE_AD-7.6 test prep is recognized as the most representative and advanced study materials among the same kinds of products. Whether the qualities and functions or the service of our NSE5_SSE_AD-7.6 Exam Questions, are leading and we boost the most professional expert team domestically.

>> New NSE5_SSE_AD-7.6 Test Sims <<

Valid Test NSE5_SSE_AD-7.6 Vce Free, Test Certification NSE5_SSE_AD-7.6 Cost

We believe that the best brands are those that go beyond expectations. They don't just do the job – they go deeper and become the

fabric of our lives. Our product boosts many merits and functions. You can download and try out our NSE5_SSE_AD-7.6 test question freely before the purchase. You can use our product immediately after you buy our product. We provide 3 versions for you to choose and you only need 20-30 hours to learn our NSE5_SSE_AD-7.6 Training Materials and prepare the exam. The passing rate and the hit rate are both high.

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	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.
Topic 3	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 4	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.
Topic 5	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q10-Q15):

NEW QUESTION # 10
Which three reports are valid report types in FortiSASE? (Choose three.)

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

Answer: A,B,D

Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25training materials, FortiSASE leverages a cloud-native FortiAnalyzer instance to provide specialized reports. These reports are designed to give administrators visibility into remote user behavior, endpoint health, and cloud application usage.
The three valid and standard report types available directly within the FortiSASE portal are:
* Web Usage Summary Report (Option A):This report provides a high-level overview of web activity across the SASE deployment. It categorizes traffic by website categories (e.g., Social Media, Streaming, Malicious Sites), top users by bandwidth, and blocked requests, helping IT teams understand how internet resources are being consumed by remote workers.
* Vulnerability Assessment Report (Option C):Since FortiSASE integrates with FortiClient and an embedded EMS, it can aggregate vulnerability scan data from managed endpoints. This report lists software vulnerabilities found on user devices (OS-level and application-level), providing a "Security Rating" or posture assessment that is critical for Zero Trust Network Access (ZTNA) enforcement.
* Shadow IT Report (Option D):Leveraging the built-inCASB (Cloud Access Security Broker) capabilities, this report identifies "unsanctioned" or "risky" SaaS applications being used by employees.
It helps organizations discover hidden security risks by cataloging cloud applications that have not been explicitly approved by the IT department.
Why other options are incorrect:
* Endpoint Compliance Deviation Report (Option B):While FortiSASE performs compliance checks via ZTNA tags, this specific name is not a standard "Report Type" template in the portal; compliance is typically monitored via theEndpoint ManagementorZTNA Dashboards.
* Cyber Threat Assessment (Option E):TheCyber Threat Assessment Program (CTAP)is a specific Fortinet sales and auditing tool

used to generate a one-time report on a network's security posture (often used for FortiGate evaluations). It is not a native, recurring report type within the day-to-day FortiSASE administration interface.

NEW QUESTION # 11
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 provides a vulnerability summary, identifies affected endpoints, and supports automatic patching for eligible vulnerabilities.
- C. It displays only critical vulnerabilities, requires manual patching for all endpoints, and does not allow viewing of affected endpoints.
- D. It shows vulnerabilities only for applications and requires endpoint users to manually check for affected endpoints.

Answer: B

Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - 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 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 down into 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 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 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 # 12
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. You can select the outsessions hash mode with all strategies that allow load balancing.
- C. When applicable, FortiGate load balances traffic through all members that meet the SLA target.
- D. SD-WAN load balancing is possible only when using the manual and the best quality strategies.

Answer: B,C

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 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, theLowest 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 identifiesall 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 forManual andLowest Cost (SLA)strategies in 7.6), the administrator must define ahash modeto 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) forall strategieswhere load- balancing is enabled.
Why other options are incorrect:
* Option B and C: These options are too restrictive. InFortiOS 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 thatManualandLowest Cost

(SLA)are the primary strategies that support the explicit load-balance toggle to steer traffic through multiple healthy members simultaneously.

NEW QUESTION # 13
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

Explanation:
According to theFortiSASE 7.6 Architecture GuideandFCP - FortiSASE 24/25 Administratormaterials, 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, andSSL Inspectionin 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 throughZTNA (Zero Trust Network Access)for session-based security or throughSD-WAN integrationwhere FortiSASE acts as a spoke to an existing corporate SD- WAN hub.
* SaaS Security:FortiSASE utilizesInline-CASBandShadow IT visibilityto 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".

NEW QUESTION # 14
Refer to the exhibit, which shows the SD-WAN rule status and configuration.

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority:2
      Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
      link-cost-factor(packet loss), link-cost-threshold(0), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, packet loss: 12.000%, selected
     Src address(1):
          10.0.1.0-10.0.1.255

     Dst address(1):
          10.0.0.0-10.255.255.255

branch1_fgt (service) # show
config service
     edit 3
          set name "Corp"
          set mode priority
          set dst "Corp-net"
          set src "LAN-net"
          set health-check "HUB1_HC"
          set link-cost-factor packet-loss
          set link-cost-threshold 0
          set priority-members 6 4 5
     next
```

Based on the exhibit, which change in the measured packet loss will make HUB1-VPN3 the new preferred member? (Choose one answer)

- A. When HUB1-VPN1 has 4% packet loss
- B. When HUB1-VPN1 has 12% packet loss
- C. When HUB1-VPN3 has 4% packet loss
- D. When all three members have the same packet loss

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, the selection process for theBest Quality (priority)strategy depends on two primary factors: the measured link quality metric and the configured member priority order.
Based on the provided exhibit (image_b40dfc.png), we can determine the following:
* Strategy and Metric: The rule is in Mode(priority) (Best Quality) using link-cost-factor(packet loss).
* Strict Comparison: The link-cost-threshold is set to0. This means there is no "advantage" given to the current preferred link; the FortiGate performs a strict comparison where the link with the objectively best metric is chosen.
* Tie-Breaker Logic: When multiple links have thesamepacket loss, the FortiGate uses theMember Priority Orderdefined in the rule (set priority-members 6 4 5) as the tie-breaker.
* Member 6 (HUB1-VPN3)is the highest priority.
* Member 4 (HUB1-VPN1)is the second priority.
* Member 5 (HUB1-VPN2)is the lowest priority.
* Current State: HUB1-VPN1 is currently selected because its packet loss (2.000%) is lower than HUB1-VPN2 (4.000%) and HUB1-VPN3 (12.000%). Even though HUB1-VPN3 has a higher configuration priority, its significantly higher packet loss prevents it from being chosen.
Evaluation of Options:
* Option A (Verified): If all three members have thesame packet loss(e.g., they all show 2%), the quality metrics are equal. The SD-WAN engine then refers to the priority-members list. Since HUB1- VPN3 (Seq 6) is the first member in that list, it will immediately become the new preferred member.
* Option B: If HUB1-VPN1 reaches 4%, it matches HUB1-VPN2 (4%). HUB1-VPN3 remains at 12%.
The system will choose between VPN1 and VPN2. Since VPN1 (Seq 4) is higher in the priority list than VPN2 (Seq 5), HUB1-VPN1 stays preferred.
* Option C: If HUB1-VPN1 reaches 12%, it matches HUB1-VPN3. However, HUB1-VPN2 is still better at4.000%. Therefore, HUB1-VPN2 would become the new preferred member, not HUB1-VPN3.

* Option D: If HUB1-VPN3 drops to 4%, it matches HUB1-VPN2. However, HUB1-VPN1 is still the best link at2.000%, so it remains selected.

NEW QUESTION # 15

......

Compared with those practice materials which are to no avail and full of hot air, our NSE5_SSE_AD-7.6 guide tests outshine them in every aspect. If you make your decision of them, you are ready to be thrilled with the desirable results from now on. All exam candidates are awfully sure of our NSE5_SSE_AD-7.6 practice materials and when they meet other needs of the exam, they would rather be our regular buyers. We are sure of anyone who wants to pass the exam as well as our NSE5_SSE_AD-7.6 question materials. We will continue making our sublime materials more useful by keeping adding useful knowledge of this exam into them.