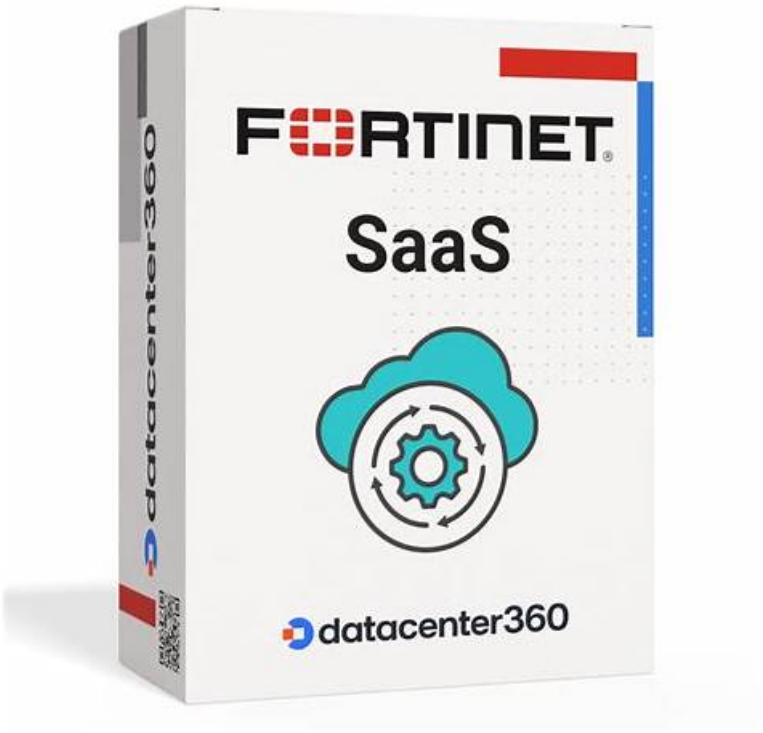
Reliable Fortinet NSE5_SSE_AD-7.6 Braindumps Ppt | NSE5_SSE_AD-7.6 Top Exam Dumps



We update our NSE5_SSE_AD-7.6 test prep within one year and you will download free which you need. After one year, we provide the client 50% discount benefit if buyers want to extend their service warranty so you can save much money. If you are the old client, you can enjoy some certain discount when buying NSE5_SSE_AD-7.6 Exam Torrent so you can enjoy more service and more benefits. Our update can provide the latest and most useful NSE5_SSE_AD-7.6 prep torrent to you and you can learn more and pass the NSE5_SSE_AD-7.6 exam successfully.

With a vast knowledge in the field, Pass4cram is always striving hard to provide actual, authentic Fortinet Exam Questions so that the candidates can pass their Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam in less time. Pass4cram tries hard to provide the best Fortinet NSE5_SSE_AD-7.6 dumps to reduce your chances of failure in the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam. Pass4cram provides an exam scenario with its Fortinet NSE5_SSE_AD-7.6 practice test (desktop and web-based) so the preparation of the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam questions becomes quite easier.

>> Reliable Fortinet NSE5_SSE_AD-7.6 Braindumps Ppt <<

Sharpen Your Time Management Skills with Fortinet NSE5_SSE_AD-7.6 Practice Test

When you decide to pass NSE5_SSE_AD-7.6 exam, you must want to find a good study materials to help you prepare for your exam. If you decide to choice our products as your study tool, you will be easier to pass your exam and get the NSE5_SSE_AD-7.6 certification in the shortest time. So do not hesitate and buy our NSE5_SSE_AD-7.6 Test Torrent, an unexpected surprise is awaiting you, we believe you will prefer to our NSE5_SSE_AD-7.6 test questions than other study materials. In order to let you understand our NSE5_SSE_AD-7.6 exam prep in detail, we are going to introduce our products to you.

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	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.
Topic 3	• 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 4	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.
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 (Q22-Q27):

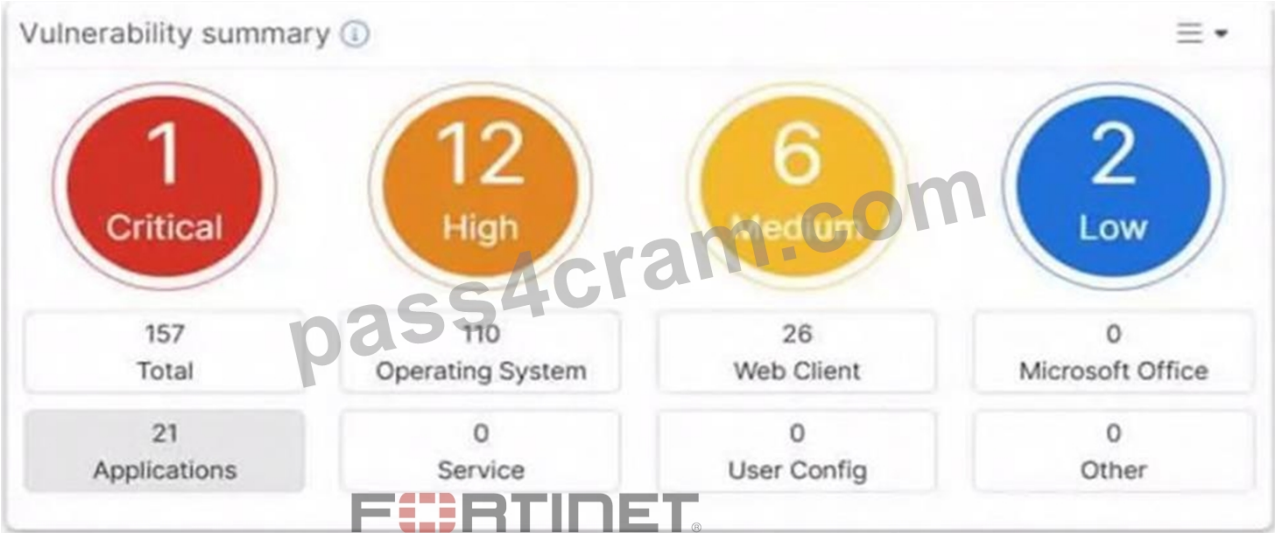
NEW QUESTION # 22
You want FortiGate to use SD-WAN rules to steer local-out traffic.
Which two constraints should you consider? (Choose two.)

- A. By default, local-out traffic does not use SD-WAN.
- B. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
- C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
- D. You must configure each local-out feature individually to use SD-WAN.

Answer: A,D

Explanation:
By default, local-out traffic does not use SD-WAN → FortiGate normally sends local-out traffic (e.g., DNS, NTP, FortiGuard updates) directly through its interfaces without applying SD-WAN rules.
You must configure each local-out feature individually to use SD-WAN → To steer local-out traffic via SD-WAN, you must explicitly configure the desired local-out features (e.g., DNS, FortiGuard, CAPWAP) to use SD-WAN rules.

NEW QUESTION # 23
Refer to the exhibit. Which two statements about the Vulnerability summary dashboard in FortiSASE are correct? (Choose two.)



- A. Automatic vulnerability patching can be enabled for supported 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. The dashboard shows the vulnerability score for unknown applications.

Answer: A,C

Explanation:
FortiSASE supports automatic patching for certain applications, and this capability is reflected in the vulnerability management workflow.
The Vulnerability summary dashboard provides drill-down visibility, including CVE data and severity details for detected vulnerabilities.

NEW QUESTION # 24
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 passively monitors the member if ICMP traffic is passing through the member.
- C. FortiGate passively monitors the member if TCP traffic is passing through the member.
- D. During passive monitoring, the SLA performance rule cannot detect dead members.
- E. FortiGate can offload the traffic that is subject to passive monitoring to hardware.

Answer: C,D

Explanation:
In theSD-WAN 7.6 Core Administratorcurriculum, the "Prefer Passive" probe mode is a hybrid monitoring strategy designed to minimize the overhead of synthetic traffic (probes) while maintaining link health visibility. According to theFortiOS 7.6 Administration Guideand theSD-WAN Study Guide, the behavior and impacts are as follows:
* TCP Traffic Requirement (Option E):Passive monitoring relies on the FortiGate's ability to inspect actual user traffic to calculate health metrics such as Latency, Jitter, and Packet Loss. Specifically, it usesTCP traffic(by analyzing TCP sequence numbers and timestamps to calculate Round Trip Time - RTT). If user traffic is flowing through the member interface, the FortiGate uses those real-world sessions for SLA calculations instead of sending its own probes.
* Inability to Detect Dead Members (Option C):A significant limitation of passive monitoring is that it cannot distinguish between a "dead" link and an "idle" link. If there is no traffic, the passive monitor has no data to analyze. Consequently, while in passive mode, the SD-WAN enginecannot detect a dead member. To mitigate this, "Prefer Passive" includes a fail-safe: if no traffic is detected for a specific period (typically3 minutes), the FortiGate will automatically switch toActive mode(sending ICMP/TCP pings) to verify if the link is actually alive.
Why other options are incorrect:
* Option A:Passive monitoring generallydisables hardware offloading (ASIC)for the monitored traffic.
This is because the CPU must inspect every packet header to calculate performance metrics; if the traffic were offloaded to the Network Processor (NP), the CPU would not see the packets, rendering passive monitoring impossible.
* Option B:While active probes often use ICMP,passive monitoringis specifically designed forTCP trafficbecause the TCP protocol's ACK structure allows for accurate RTT and loss calculation without synthetic packets.
* Option D:The "3-minute" timer is actually the trigger to switchfrom passive to activewhen traffic is absent, not the fallback timer to return to passive. The fallback to passive happens as soon as valid TCP traffic is detected again.
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administratorstudy materials, FortiSASE supports three primary external (remote) authentication sources to verify the identity of remote users (SIA and SPA users). These sources allow organizations to leverage their existing identity infrastructure for seamless onboarding and policy enforcement:
* Security Assertion Markup Language (SAML) (Option A):This is the most common and recommended method for modern SASE deployments. FortiSASE acts as aSAML Service Provider (SP)and integrates withIdentity Providers (IdP)such as Microsoft Entra ID (formerly Azure AD), Okta, or FortiAuthenticator. This enables Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
* Lightweight Directory Access Protocol (LDAP) (Option C):FortiSASE can connect to on-premises or cloud-based LDAP servers (such as Windows Active Directory). This allows the administrator to map existing AD groups to FortiSASE user groups for granular security policy application.
* Remote Authentication Dial-in User Service (RADIUS) (Option E):RADIUS is supported for organizations that use centralized authentication servers or traditional MFA solutions (like RSA SecurID). FortiSASE can query a RADIUS server to validate user credentials before granting access to the SASE tunnel.
Why other options are incorrect:
* OpenID Connect (OIDC) (Option B):While OIDC is a modern authentication protocol similar to SAML, FortiSASE's primary integration for external Identity Providers is currently standardized on SAML 2.0.
* TACACS+ (Option D):Terminal Access Controller Access-Control System Plus is primarily used for administrative access(AAA)

to network devices (like logging into a FortiGate CLI or FortiManager).
It is not used for end-user VPN or SASE authentication in the Fortinet ecosystem.

NEW QUESTION # 25
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. 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. Providing secure web browsing through remote browser isolation, addressing shadow IT with zero-trust access, and protecting data at rest only.
- D. Monitoring SaaS application performance, isolating browser sessions for all websites, and integrating with SD-WAN for data loss prevention.

Answer: B

Explanation:
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.

NEW QUESTION # 26
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?

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

Answer: B

Explanation:
Before an SD-WAN member can be deleted, it must not be referenced anywhere. The most common blocking reference is in Performance SLA definitions. Removing the member from all SLA profiles is the required first step before the system will allow deletion.

NEW QUESTION # 27
.....

□ Open □ www.pdfvce.com □ and search for ➥ NSE5_SSE_AD-7.6 □ to download exam materials for free □ □NSE5_SSE_AD-7.6 Discount Code

- Dump NSE5_SSE_AD-7.6 Torrent □ NSE5_SSE_AD-7.6 Test Assessment □ NSE5_SSE_AD-7.6 Latest Exam Cost □ Search for （ NSE5_SSE_AD-7.6 ） and easily obtain a free download on [www.troytecdumps.com] □ □100% NSE5_SSE_AD-7.6 Accuracy
- New NSE5_SSE_AD-7.6 Dumps Book □ NSE5_SSE_AD-7.6 Exam Discount Voucher □ Valid NSE5_SSE_AD-7.6 Test Topics □ Search for ➥ NSE5_SSE_AD-7.6 □ and download exam materials for free through □ www.pdfvce.com □ □Exam Vce NSE5_SSE_AD-7.6 Free
- Fortinet NSE5_SSE_AD-7.6 PDF Questions – Ideal Material for Quick Preparation □ Easily obtain free download of ➤ NSE5_SSE_AD-7.6 □ by searching on □ www.vceengine.com □ □New NSE5_SSE_AD-7.6 Test Test
- New NSE5_SSE_AD-7.6 Dumps Book □ Examcollection NSE5_SSE_AD-7.6 Dumps □ NSE5_SSE_AD-7.6 Test Assessment □ Enter □ www.pdfvce.com □ and search for ➽ NSE5_SSE_AD-7.6 □ to download for free □ □NSE5_SSE_AD-7.6 Latest Guide Files
- Fortinet NSE5_SSE_AD-7.6 PDF Questions – Ideal Material for Quick Preparation □ Open ➠ www.exam4labs.com □ □ and search for ☀ NSE5_SSE_AD-7.6 □☀□ to download exam materials for free □NSE5_SSE_AD-7.6 Exam Discount Voucher
- Hot Reliable NSE5_SSE_AD-7.6 Braindumps Ppt | Authoritative NSE5_SSE_AD-7.6 Top Exam Dumps and Updated Practice Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Tests □ Search for { NSE5_SSE_AD-7.6 } and download it for free immediately on ➡ www.pdfvce.com □□□ □NSE5_SSE_AD-7.6 Online Training
- 2026 Updated Reliable NSE5_SSE_AD-7.6 Braindumps Ppt | 100% Free Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Top Exam Dumps □ Search for □ NSE5_SSE_AD-7.6 □ and obtain a free download on ☀ www.practicevce.com □☀□ □NSE5_SSE_AD-7.6 Latest Test Bootcamp
- Try Approved Fortinet NSE5_SSE_AD-7.6 Exam Questions To Pass NSE5_SSE_AD-7.6 Exam □ The page for free download of □ NSE5_SSE_AD-7.6 □ on 「 www.pdfvce.com 」 will open immediately □NSE5_SSE_AD-7.6 Latest Guide Files
- Types of www.vce4dumps.com Fortinet NSE5_SSE_AD-7.6 Practice Questions □ Search for □ NSE5_SSE_AD-7.6 □ and download it for free immediately on ▷ www.vce4dumps.com ◁ □NSE5_SSE_AD-7.6 Free Dumps
- www.stes.tyc.edu.tw, class.most-d.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, eduderma.info, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes