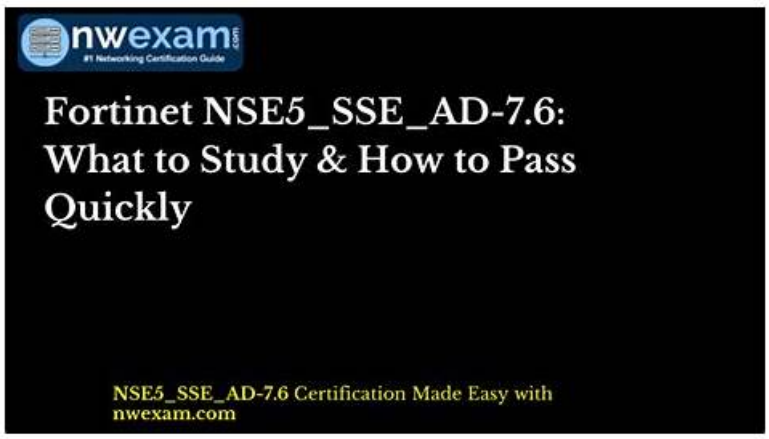
NSE5_SSE_AD-7.6 Vce Torrent, NSE5_SSE_AD-7.6 Reliable Braindumps Book



The PracticeDump is a leading platform that offers real, valid, and subject matter expert's verified NSE5_SSE_AD-7.6 exam questions. These NSE5_SSE_AD-7.6 exam practice questions are particularly designed for fast Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam preparation. The PracticeDump NSE5_SSE_AD-7.6 exam questions are designed and verified by experienced and qualified Fortinet NSE5_SSE_AD-7.6 Exam trainers. They work together and put all their expertise and experience to ensure the top standard of PracticeDump NSE5_SSE_AD-7.6 exam practice questions all the time.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.
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	• 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	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.

>> NSE5_SSE_AD-7.6 Vce Torrent <<

NSE5_SSE_AD-7.6 Reliable Braindumps Book & NSE5_SSE_AD-7.6 Valid Dumps Files

As long as you are willing to exercise on a regular basis, the exam will be a piece of cake, because what our NSE5_SSE_AD-7.6 practice questions include are quintessential points about the exam. They are almost all the keypoints and the latest information contained in our NSE5_SSE_AD-7.6 Study Materials that you have to deal with in the real exam. And we have high pass rate of our NSE5_SSE_AD-7.6 exam questions as 98% to 100%. It is hard to find in the market.

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

Questions (Q32-Q37):

NEW QUESTION # 32
Which statement is true about FortiSASE supported deployment?

- A. FortiSASE supports VPN mode and Agentless mode, based on user requirements.
- B. FortiSASE relies on ZTNA-only mode, which replaces SWG and endpoint functions.
- C. FortiSASE supports both Endpoint mode and SWG mode, depending on deployment.
- D. FortiSASE operates only in SWG mode, where all traffic is forced through FortiSASE POPs.

Answer: C

Explanation:
FortiSASE supports multiple deployment options, including Endpoint mode (using FortiClient) and SWG mode (agentless), allowing organizations to choose the method that best fits their access and security requirements.

NEW QUESTION # 33
How is the Geofencing feature used in FortiSASE? (Choose one answer)

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

Answer: D

NEW QUESTION # 34
Which three reports are valid report types in FortiSASE? (Choose three.)

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

Answer: A,C,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 # 35
You have configured the performance SLA with the probe mode as Prefer Passive.
What are two observable impacts of this configuration? (Choose two.)

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

Answer: A,E

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 # 36
Which statement is true about scheduling a FortiClient upgrade using an endpoint upgrade rule?

- A. Scheduled upgrades automatically reboot macOS endpoints after installation.

- B. When scheduled, the installation always starts immediately if the endpoint is online.
- C. An endpoint upgrade rule can be assigned to a user group.
- D. If the scheduled time is already past in the local time zone of the endpoint, installation starts the next day at that time.

Answer: D

Explanation:
A scheduled FortiClient upgrade is executed according to the endpoint's local time. If the scheduled time has already passed in that time zone, the upgrade is deferred until the same time on the following day.

NEW QUESTION # 37
.....

Some candidates may wonder that if the payment is quite complex and hard, in fact it is quite easy and simple. Once you have selected the NSE5_SSE_AD-7.6 study materials, please add them to your cart. Then when you finish browsing our web pages, you can directly come to the shopping cart page and submit your orders of the NSE5_SSE_AD-7.6 learning quiz. Our payment system will soon start to work. Then certain money will soon be deducted from your credit card to pay for the NSE5_SSE_AD-7.6 preparation questions. And we will send them to you in 5 to 10 minutes after your purchase.