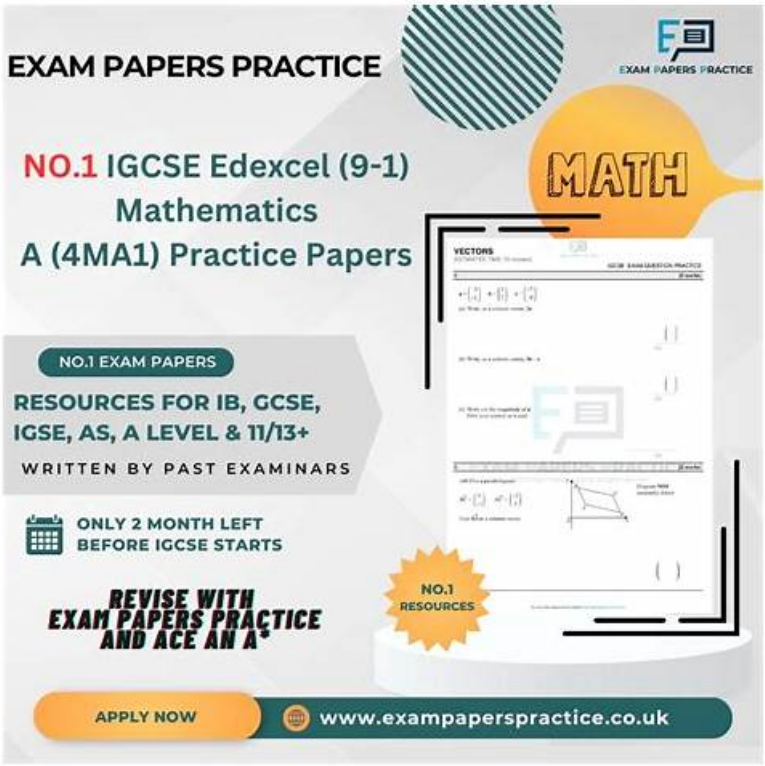
NSE5_SSE_AD-7.6 Valid Exam Papers & Reliable NSE5_SSE_AD-7.6 Exam Cost



2026 Latest TestInsides NSE5_SSE_AD-7.6 PDF Dumps and NSE5_SSE_AD-7.6 Exam Engine Free Share: https://drive.google.com/open?id=1yba3M2cqoe-3RLz-RLiTmsXcQlBlXgzu

Our users are all over the world and they have completed their exams through the help of our NSE5_SSE_AD-7.6 study guide. As you can see the feedbacks from our loyal customers, all of them are grateful to our NSE5_SSE_AD-7.6 exam braindumps and become successful people with the NSE5_SSE_AD-7.6 Certification. And what are you waiting for? Just selecting our NSE5_SSE_AD-7.6 learning materials, the next one to get an international certificate is you!

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

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

Up-to-Date Fortinet NSE5_SSE_AD-7.6 Exam Questions For Best Result

We know deeply that a reliable NSE5_SSE_AD-7.6 exam material is our company's foothold in this competitive market. High accuracy and high quality are the most important things we always looking for. Compared with the other products in the market, our NSE5_SSE_AD-7.6 latest questions grasp of the core knowledge and key point of the real exam, the targeted and efficient NSE5_SSE_AD-7.6 study training dumps guarantee our candidates to pass the test easily. Passing exam won't be a problem anymore as long as you are familiar with our NSE5_SSE_AD-7.6 exam material (only about 20 to 30 hours practice).

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q21-Q26):

NEW QUESTION # 21
Which three reports are valid report types in FortiSASE? (Choose three.)

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

Answer: C,D,E

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 # 22
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 TCP traffic is passing through the member.
- C. FortiGate passively monitors the member if ICMP 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: B,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 # 23
Which three FortiSASE use cases are possible? (Choose three answers)

- A. Secure Internet Access (SIA)
- B. Secure VPN Access (SVA)
- C. Secure Private Access (SPA)
- D. Secure Browser Access (SBA)
- E. Secure SaaS Access (SSA)

Answer: A,C,E

NEW QUESTION # 24
Which two methods are available for provisioning FortiClient on endpoints using FortiSASE?
(Choose two.)

- A. FortiClient can be provisioned using installers with an invitation code from the FortiSASE portal, SCCM or GPO, or

mobile device management (MDM) software.

- B. FortiClient provisioning is limited to using mobile device management MDM software or manual installation without requiring an invitation code.
- C. FortiClient can be provisioned using SCCM or GPO, but only through an external portal, not the FortiSASE portal.
- D. FortiClient can be provisioned only by distributing installers to end users through the FortiSASE portal without an invitation code.
- E. FortiClient can be provisioned by distributing the installer to end users for manual installation.

Answer: A,E

Explanation:
Administrators can distribute the FortiClient installer for manual installation on endpoints.
FortiClient can also be provisioned using installers embedded with an invitation code, distributed through SCCM, GPO, or MDM solutions via the FortiSASE portal.

NEW QUESTION # 25
Refer to the exhibit.

You want the performance service-level agreement (SLA) to measure the jitter of each member. Which configuration change must you make to achieve this result?

- A. Add an SLA target and define a jitter threshold.
- B. Set the protocol to HTTP.
- C. Specify the participant members.
- D. No change is required.

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide andFortiOS 7.6 Administration Guide, no configuration change is required to simplymeasurejitter.
* Implicit Measurement: In FortiOS, once a Performance SLA (Health Check) is configured with an Activeprobe mode (as seen in the exhibit with Ping selected), the FortiGate automatically begins calculating three key quality metrics for every member interface:Latency,Jitter, andPacket Loss.
* Visibility: Even without an SLA Target defined, these real-time measurements are visible in theSD- WAN Monitorand via the CLI command diagnose sys virtual-wan-link health-check <SLA_Name>.
* Active Probes: Because the probe mode is set toActiveusing thePingprotocol, the FortiGate sends synthetic packets at the definedCheck interval(500ms in the exhibit). It calculates jitter by measuring the variation in the round-trip time (RTT) between these consecutive probes.
Why other options are incorrect:
* Option B: Adding anSLA targetand defining a jitter threshold is only necessary if you want the SD- WAN engine to makesteering decisionsbased on that metric (e.g., "remove this link from the pool if jitter exceeds 50ms"). It is not required just tomeasurethe jitter.
* Option C: While you can specify participants, the current setting is "All SD-WAN Members," which means it is already measuring jitter for every member.
* Option D:HTTPis an alternative probe protocol, butPing (ICMP)is perfectly capable of measuring jitter and is often preferred for its lower overhead.

NEW QUESTION # 26
.....

Nowadays the knowledge capabilities and mental labor are more valuable than the manual labor because knowledge can create more wealth than the mental labor. If you boost professional knowledge capabilities in some area you are bound to create a lot of values and can get a good job with high income. Passing the test of NSE5_SSE_AD-7.6 Certification can help you achieve that, and our NSE5_SSE_AD-7.6 training materials are the best study materials for you to prepare for the NSE5_SSE_AD-7.6 test. Our NSE5_SSE_AD-7.6 guide materials combine the key information to help the clients both solidify the foundation and advance with the times.

download □New NSE5_SSE_AD-7.6 Exam Objectives

- Valid Fortinet Valid Exam Papers – High-quality Reliable NSE5_SSE_AD-7.6 Exam Cost □ Search on ✔ www.pdfvce.com □✔□ for ☀ NSE5_SSE_AD-7.6 □☀□ to obtain exam materials for free download □ □NSE5_SSE_AD-7.6 Flexible Testing Engine
- Fortinet - Reliable NSE5_SSE_AD-7.6 Valid Exam Papers □ Search for ☀ NSE5_SSE_AD-7.6 □☀□ and obtain a free download on " www.vce4dumps.com " □NSE5_SSE_AD-7.6 Valid Test Vce Free
- Quiz 2026 Fortinet - NSE5_SSE_AD-7.6 - Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Valid Exam Papers □ Open ☀ www.pdfvce.com □☀□ enter 【 NSE5_SSE_AD-7.6 】 and obtain a free download □ □Pass4sure NSE5_SSE_AD-7.6 Pass Guide
- Test NSE5_SSE_AD-7.6 Questions Fee □ Test NSE5_SSE_AD-7.6 Questions Fee □ Practice NSE5_SSE_AD-7.6 Mock □ Immediately open ➠ www.easy4engine.com □ and search for □ NSE5_SSE_AD-7.6 □ to obtain a free download □Reliable NSE5_SSE_AD-7.6 Braindumps Ebook
- amiexmif142294.blogoxo.com, www.jkkdh.com, nikolasydpv058635.59bloggers.com, aliciadnos262891.blogaritma.com, 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, adreafdcg940642.blogofchange.com, 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, prestonogep454115.empirewiki.com, learn-school.webtemplates.in, privatebookmark.com, Disposable vapes

P.S. Free 2026 Fortinet NSE5_SSE_AD-7.6 dumps are available on Google Drive shared by TestInsides: https://drive.google.com/open?id=1yba3M2cqoe-3RLz-RLiTmsXcQlBlXgzu