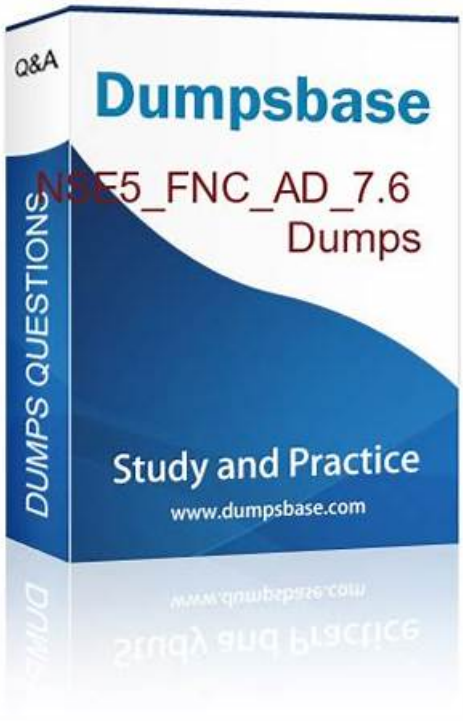
Valid Dumps NSE5_SSE_AD-7.6 Book & NSE5_SSE_AD-7.6 Latest Exam Pattern



NSE5_SSE_AD-7.6 certification can demonstrate your mastery of certain areas of knowledge, which is internationally recognized and accepted by the general public as a certification. NSE5_SSE_AD-7.6 certification is so high that it is not easy to obtain it. It requires you to invest time and energy. If you are not sure whether you can strictly request yourself, our NSE5_SSE_AD-7.6 Exam Training can help you. Help is to arrange time for you and provide you with perfect service. If you use our learning materials to achieve your goals, we will be honored. NSE5_SSE_AD-7.6 exam prep look forward to meeting you.

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

>> Valid Dumps NSE5_SSE_AD-7.6 Book <<

NSE5_SSE_AD-7.6 Latest Exam Pattern | NSE5_SSE_AD-7.6 Upgrade Dumps

If you want to avoid being eliminated by machine, you must constantly improve your ability in all aspects. The emergence of NSE5_SSE_AD-7.6 dumps torrent provides you with a very good chance to improve yourself. On the one hand, our NSE5_SSE_AD-7.6 quiz torrent can help you obtain professional certificates with high quality in any industry without any difficulty. On the other hand, NSE5_SSE_AD-7.6 Exam Guide can give you the opportunity to become a senior manager of the company, so that you no longer engage in simple and repetitive work, and you will never face the threat of layoffs.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q45-Q50):

NEW QUESTION # 45
How is the Geofencing feature used in FortiSASE? (Choose one answer)

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

Answer: B

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 # 46
Which three reports are valid report types in FortiSASE? (Choose three.)

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

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 # 47
Which secure internet access (SIA) use case minimizes individual endpoint configuration?

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

Answer: A

Explanation:
Agentless remote user internet access uses an explicit proxy PAC file, which minimizes configuration on individual endpoints because no FortiClient agent installation or per-device setup is required.

NEW QUESTION # 48
You want FortiGate to use SD-WAN rules to steer local-out traffic.
Which two constraints should you consider? (Choose two.)

- A. You must configure each local-out feature individually to use SD-WAN.
- B. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
- C. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
- D. By default, local-out traffic does not 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 # 49
You have a FortiGate configuration with three user-defined SD-WAN zones and one or two members in each of these zones. One SD-WAN member is no longer used in health-check and SD-WAN rules. This member is the only member of its zone. You want to

delete it.
What happens if you delete the SD-WAN member from the FortiGate GUI?

- A. FortiGate displays an error message. SD-WAN zones must contain at least one member.
- B. FortiGate accepts the deletion and removes static routes as required.
- C. FortiGate accepts the deletion and places the member in the default SD-WAN zone.
- D. FortiGate accepts the deletion with no further action.

Answer: B

Explanation:
In FortiOS, you can remove an SD-WAN member from the GUI as long as it is not in use in any health-checks, SD-WAN rules, or policies.
When you delete it, FortiGate will automatically clean up related routes (static or dynamic SD- WAN routes referencing that member).

NEW QUESTION # 50
.....