Fortinet NSE5_SSE_AD-7.6 Reliable Exam Cram - NSE5_SSE_AD-7.6 Latest Exam Test

Our company has employed a lot of leading experts in the field to compile the NSE5_SSE_AD-7.6 exam question. Our system of team-based working is designed to bring out the best in our people in whose minds and hands the next generation of the best NSE5_SSE_AD-7.6 exam torrent will ultimately take shape. Our company has a proven track record in delivering outstanding after sale services and bringing innovation to the guide torrent. Your success is guaranteed for our experts can produce world class NSE5_SSE_AD-7.6 Guide Torrent for our customers. You will be bound to pass the NSE5_SSE_AD-7.6 exam.

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

>> Fortinet NSE5_SSE_AD-7.6 Reliable Exam Cram <<

Fortinet NSE5_SSE_AD-7.6 Latest Exam Test - NSE5_SSE_AD-7.6 Reliable Test Guide

You final purpose is to get the NSE5_SSE_AD-7.6 certificate. So it is important to choose good NSE5_SSE_AD-7.6 study materials. In fact, our aim is the same with you. Our NSE5_SSE_AD-7.6 learning questions have strong strengths to help you pass the exam. Maybe you still have doubts about our NSE5_SSE_AD-7.6 Exam Braindumps. We have statistics to prove the truth that the pass rate of our NSE5_SSE_AD-7.6 practice engine is 98% to 100%.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q19-Q24):

NEW QUESTION # 19
Which three reports are valid report types in FortiSASE? (Choose three.)

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

Answer: A,B,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 # 20
The IT team is wondering whether they will need to continue using MDM tools for future FortiClient upgrades.
What options are available for handling future FortiClient upgrades?

- A. Perform onboarding for managed endpoint users with a newer FortiClient version.
- B. Enable the Endpoint Upgrade feature on the FortiSASE portal.
- C. A newer FortiClient version will be auto-upgraded on demand.
- D. FortiClient will need to be manually upgraded.

Answer: B

Explanation:
According to theFortiSASE 7.6 Feature Administration Guideand the latest updates to theNSE 5 SASE curriculum, FortiSASE has introduced native lifecycle management for FortiClient agents to reduce the operational burden on IT teams who previously relied solely on third-party MDM (Mobile Device Management) or GPO (Group Policy Objects) for every update.
TheEndpoint Upgradefeature, found underSystem > Endpoint Upgradein the FortiSASE portal, allows administrators to perform the following:

* Centralized Version Control: Administrators can see which versions are currently deployed and which "Recommended" versions are available from FortiGuard.
* Scheduled Rollouts: You can choose to upgrade all endpoints or specific endpoint groups at a designated time, ensuring that upgrades do not disrupt business operations.
* Status Monitoring: The portal provides a real-time dashboard showing the progress of the upgrade (e.
g.,Downloading,Installing,Reboot Pending, orSuccess).
* Manual vs. Managed: While MDM is still highly recommended for theinitial onboarding(the first time FortiClient is installed and connected to the SASE cloud), all subsequent upgrades can be handled natively by the FortiSASE portal.
Why other options are incorrect:
* Option B: Manual upgrades are inefficient for large-scale deployments (~400 users in this scenario) and are not the intended "feature-rich" solution provided by FortiSASE.
* Option C: "Onboarding" refers to the initial setup. Re-onboarding every time a version changes would be redundant and counterproductive.
* Option D: While the system canmanagethe upgrade, it is not "auto-upgraded on demand" by the client itself without administrative configuration in the portal. The administrator must still define the target version and schedule.

NEW QUESTION # 21
Which two delivery methods are used for installing FortiClient on a user's laptop? (Choose two.)

- A. Configure automatic installation through an API to the user's laptop.
- B. Download the installer directly from the FortiSASE portal.
- C. Use zero-touch installation through a third-party application store.
- D. Send an invitation email to selected users containing links to FortiClient installers.

Answer: B,D

Explanation:
TheFortiSASE 7.6 Administration Guideoutlines the standard onboarding procedures for deploying the FortiClientagent to remote endpoints. There are two primary user-facing delivery methods:
* Download from the FortiSASE portal (Option B):Administrators can provide users with access to the FortiSASE portal where they can directly download apre-configured installer. This installer is uniquely tied to the organization's SASE instance, ensuring the client automatically registers to the correct cloud EMS upon installation.
* Invitation Email (Option C):This is the most common administrative method. The FortiSASE portal (via its integrated EMS) allows administrators to send an invitation email to specific users or groups.
This email contains direct download links for various operating systems (Windows, macOS, Linux) and the necessary invitation code for zero-touch registration.
Why other options are incorrect:
* Option A:While third-party stores (like the App Store or Google Play) are used for mobile devices, "zero-touch installation through a third-party store" is not the standard curriculum-defined method for laptops(Windows/macOS) in a SASE environment.
* Option D:FortiSASE does not use a direct "API to the user's laptop" for automatic installation. While MDM/GPO (centralized deployment) is supported, it is not described as an API-based auto-installation in the core curriculum.

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.)

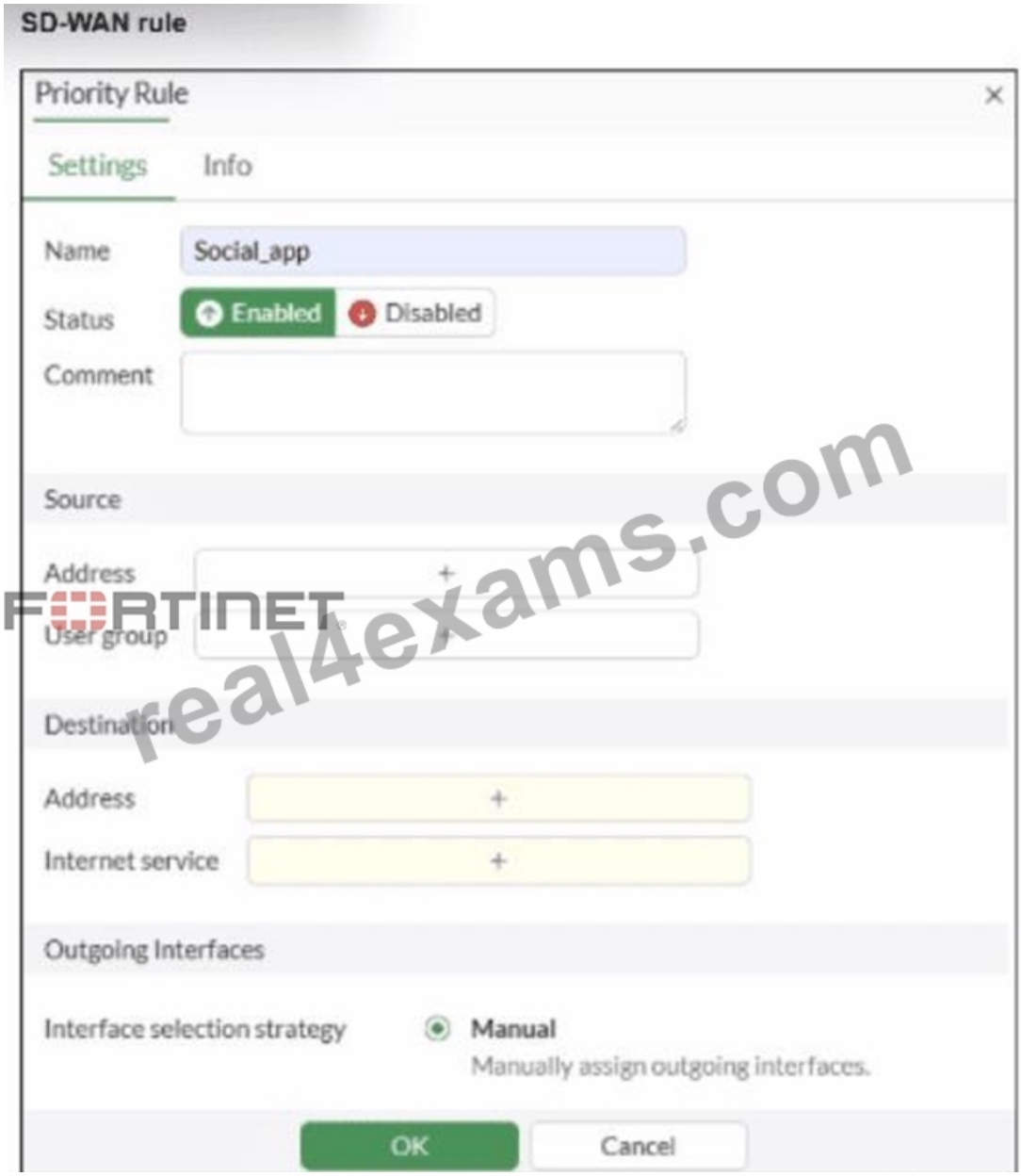
- A. FortiGate passively monitors the member if TCP traffic is passing through the member.
- B. FortiGate passively monitors the member if ICMP traffic is passing through the member.
- C. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.
- D. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
- 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 # 23
Refer to the exhibit.



You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link. What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

- A. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.
- B. Install a license to allow applications as destinations of SD-WAN rules.
- C. Enable the visibility of the applications field as destinations of the SD-WAN rule.
- D. In the Internet service field, select Facebook and LinkedIn.

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorcurriculum and theFortiOS 7.6 Administration Guide, setting common web-based services like Facebook and LinkedIn as destinations in an SD-WAN rule is primarily accomplished through theInternet Service Database (ISDB).
* Internet Service vs. Application Control: In FortiOS, there is a distinction betweenInternet Services (which use a database of known IP addresses and ports to identify traffic at the first packet) and Applications(which require the IPS engine to inspect deeper into the packet flow to identify Layer 7 signatures).
* SD-WAN Efficiency: Fortinet recommends using theInternet service fieldfor services like Facebook and LinkedIn in SD-WAN rules because it allows the FortiGate to steer the traffic immediately upon the first packet. If the "Application" signatures were used instead, the first session might be misrouted because the application is not identified until after the initial handshake.
* GUI Configuration: As shown in the exhibit (image_b3a4c2.png), the "Destination" section of an SD- WAN rule includes anInternet servicefield by default. To steer Facebook and LinkedIn traffic, the administrator simply clicks the "+" icon in that field

and selects the entries for Facebook and LinkedIn from the database.
* Feature Visibility (Alternative): While youcanenable a specific "Application" field inSystem > Feature Visibility(by enabling "Application Detection Based SD-WAN"), this is typically used for less common applications that do not have dedicated ISDB entries. For the specific "applications" mentioned (Facebook and LinkedIn), they are natively available in theInternet servicefield, making Option B the most direct and common implementation.
Why other options are incorrect:
* Option A: Licensing for application signatures is part of the standard FortiGuard services and is not a prerequisite specific only to "applications as destinations" in SD-WAN rules.
* Option C: Standalone FortiGate devices fully support application-based and ISDB-based steering in SD-WAN rules.
* Option D: While enabling feature visibility would add anadditionalfield for L7 applications, it is not a "must" for Facebook and LinkedIn, which are already accessible via the Internet Service field provided in the default GUI layout.

NEW QUESTION # 24
.....

Research indicates that the success of our highly-praised NSE5_SSE_AD-7.6 test questions owes to our endless efforts for the easily operated practice system. Most feedback received from our candidates tell the truth that our NSE5_SSE_AD-7.6 guide torrent implement good practices, systems.We educate our candidates with less complicated Q&A but more essential information. And our NSE5_SSE_AD-7.6 Exam Dumps also add vivid examples and accurate charts to stimulate those exceptional cases you may be confronted with. You can rely on our NSE5_SSE_AD-7.6 test questions, and we'll do the utmost to help you succeed.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, paidforarticles.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes