Pass2Certify.com
Prepare, Practice, & Pass.

Fortinet

NSE5_SSE_AD-7.6

ExamName: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator

Exam Version: 6.1

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

https://pass2certify.com/exam/nse5_sse_ad-7.6

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Single Select)

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

Answer: A

Explanation:
According to the FortiSASE 7.6 Feature Administration Guide and the latest updates to the NSE 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.
The Endpoint Upgrade feature, found under System > Endpoint Upgrade in 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, or Success).
Manual vs. Managed: While MDM is still highly recommended for the initial 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 can manage the 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.

Question 2. (Multi Select)

SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.

Which three configuration elements must you configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

A: Firewall policies
B: Security profiles
C: Interfaces
D: Routing
E: Traffic shaping

Answer: A, C, D

Explanation:
According to the SD-WAN 7.6 Core Administrator study guide and the FortiOS 7.6 Administration Guide, for the FortiGate SD-WAN engine to successfully steer traffic using SD-WAN rules, three fundamental configuration components must be in place. This is because the SD-WAN rule lookup occurs only after certain initial conditions are met in the packet flow:
Interfaces (Option C): You must first define the physical or logical interfaces (such as ISP links, LTE, or VPN tunnels) as SD-WAN members. These members are then typically grouped into SD-WAN Zones. Without designated member interfaces, there is no "pool" of links for the SD-WAN rules to select from.
Routing (Option D): For a packet to even be considered by the SD-WAN engine, there must be a matching route in the Forwarding Information Base (FIB). Usually, this is a static route where the destination is the network you want to reach, and the gateway interface is set to the SD-WAN virtual interface (or a specific SD-WAN zone). If there is no route pointing to SD-WAN, the FortiGate will use other routing table entries (like a standard static route) and bypass the SD-WAN rule-based steering logic entirely.
Firewall Policies (Option A): In FortiOS, no traffic is allowed to pass through the device unless a Firewall Policy permits it. To steer traffic, you must have a policy where the Incoming Interface is the internal

network and the Outgoing Interface is the SD-WAN zone (or the virtual-wan-link). The SD-WAN rule selection happens during the "Dirty" session state, which requires a policy match to proceed with the session creation.

Why other options are incorrect:

Security Profiles (Option B): While mandatory for Application-level steering (to identify L7 signatures), basic SD-WAN steering based on IP addresses, ports, or ISDB objects does not require security profiles to be active.

Traffic Shaping (Option E): This is an optimization feature used to manage bandwidth once steering is already determined; it is not a prerequisite for the steering engine itself to function.

Question 3. (DRAGDROP)

In which order does a FortiGate device consider the following elements shown in the left column during the route lookup process?

Select the element in the left column, hold and drag it to a blank position in the column on the right. Place the four correct elements in order, placing the first element in the first position at the top of the column. Once you place an element, you can move it again if you want to change your answer before moving to the next question. You need to drop four elements in the work area.

Select and drag the screen divider to change the viewable area of the source and work areas.

Answer:

Question 4. (Multi Select)

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

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

Answer: A, C, D

Explanation:
According to the FortiSASE 7.6 Administration Guide and the FCP - FortiSASE 24/25 training 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-in CASB (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 the Endpoint Management or ZTNA Dashboards.
Cyber Threat Assessment (Option E): The Cyber 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.

Question 5. (Single Select)

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 with no further action.
D: FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: B

Explanation:
Questions no: 9 Verified Answer: B
Comprehensive and Detailed Explanation with all FortiSASE and SD-WAN 7.6 Core Administrator curriculum documents: According to the SD-WAN 7.6 Core Administrator study guide and FortiOS 7.6 Administration Guide, the behavior for deleting an SD-WAN member from the GUI when it is the only member in its zone is governed by the following operational logic:
Reference Checks: Before allowing the deletion of any SD-WAN member, FortiOS performs a "check for dependencies." If an interface is being used in an active Performance SLA or an SD-WAN Rule, the GUI will typically prevent the deletion or gray out the option until those references are removed. However, the

question specifies that this member is no longer used in health-checks or rules.
Zone Integrity: Unlike some other network objects, an SD-WAN zone is permitted to exist without any members. When you delete the final member of a user-defined zone through the GUI, the zone itself remains in the configuration as an empty container.
Route Management: When an SD-WAN member is deleted, any static routes that were specifically tied to that interface's membership in the SD-WAN bundle are automatically updated or removed by the FortiGate to prevent routing loops or "black-holing" traffic. This is part of the automated cleanup process handled by the FortiOS management plane.
GUI vs. CLI: In the GUI, the process is streamlined to allow the removal of the member interface. Once the member is deleted, the interface returns to being a "regular" system interface and can be used for standard firewall policies or other functions.
Why other options are incorrect:
Option A: There is no requirement that a zone must contain at least one member; "empty" zones are valid configuration objects in FortiOS 7.6.
Option C: While the deletion is accepted, it is not with "no further action"—the system must still reconcile the routing table and interface status.
Option D: FortiGate does not automatically move deleted members into the default zone (virtual-wan-link). Once deleted, the interface is simply no longer an SD-WAN member.

Need more info? Check the link below:

https://pass2certify.com/exam/nse5_sse_ad-7.6

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com