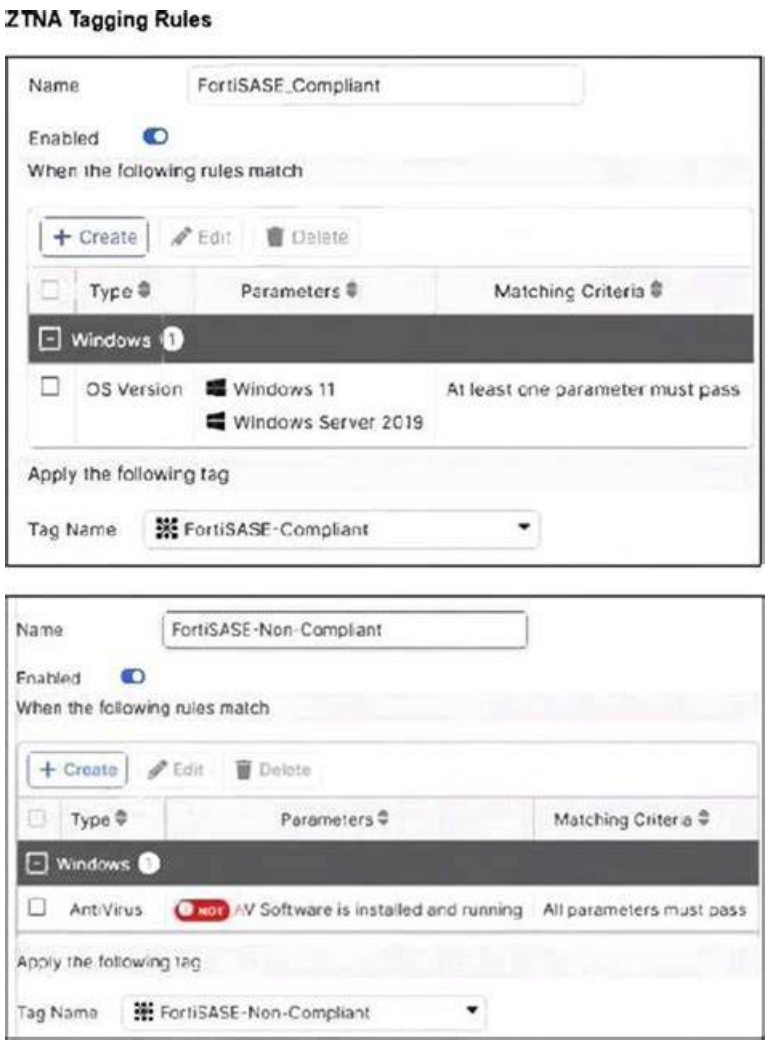
Pass Guaranteed 2026 Trustable NSE7_SSE_AD-25: Latest Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator Dumps Free



P.S. Free & New NSE7_SSE_AD-25 dumps are available on Google Drive shared by ActualTestsIT: https://drive.google.com/open?id=1BDdAM7oY45TVNJSaFHaqbkSoyvdvEp6j

The pass rate is 98% for NSE7_SSE_AD-25 exam bootcamp, and if you choose us, we can ensure you that you can pass the exam and obtain the certification successfully. In addition, NSE7_SSE_AD-25 exam materials are edited by professional experts, therefore they are high-quality, and you can improve your efficiency by using NSE7_SSE_AD-25 Exam brainidumps of us. We offer you free demo to have a try before buying NSE7_SSE_AD-25 training materials, so that you can know what the complete version is like. We have online and offline chat service for NSE7_SSE_AD-25 training materials, and if you have any questions, you can consult us.

Fortinet NSE7_SSE_AD-25 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Identity and Access Management	15-20%	- User authentication methods - Certificate-based authentication - SSO integration with identity providers - Policy-based access control

Topic 2: FortiSASE Architecture and Components	15-20%	- Components: FortiGate SASE, FortiProxy, FortiClient - SASE topology and network design - FortiSASE overview and deployment models - Zero Trust Network Access (ZTNA) fundamentals
Topic 3: Monitoring, Logging, and Troubleshooting	15-20%	- Log analysis and reporting - Diagnostic commands and tools - Performance monitoring - Common troubleshooting scenarios
Topic 4: FortiSASE Configuration and Administration	25-30%	- Tunnel mode and web proxy configurations - Security profiles and policies - Initial setup and configuration - Bandwidth and traffic management
Topic 5: Security Services	20-25%	- Web filtering and DNS filtering - Threat protection features - Sandbox integration - SSL inspection configuration

Latest Fortinet NSE7_SSE_AD-25 Training & NSE7_SSE_AD-25 Certified Questions

The design of our NSE7_SSE_AD-25 learning materials is ingenious and delicate. Every detail is perfect. For example, if you choose to study our learning materials on our windows software, you will find the interface our learning materials are concise and beautiful, so it can allow you to study NSE7_SSE_AD-25 learning materials in a concise and undisturbed environment. In addition, you will find a lot of small buttons, which can give you a lot of help. Some buttons are used to hide or show the answer. What's more important is that we have spare space, so you can take notes under each question in the process of learning NSE7_SSE_AD-25 Learning Materials.

Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator Sample Questions (Q40-Q45):

NEW QUESTION # 40
How does FortiSASE hide user information when viewing and analyzing logs? (Choose one answer)

- A. By deleting log data
- B. By hashing log data
- C. By compressing log data
- D. By tokenization in log data

Answer: B

NEW QUESTION # 41
Which two benefits come from integrating SoCaaS with FortiSASE? (Choose two answers)

- A. Provides bandwidth usage analytics
- B. Eliminates the need of endpoint projection software
- C. Continuous threat monitoring of all connected endpoints
- D. Centralized visibility of all threat events

Answer: C,D

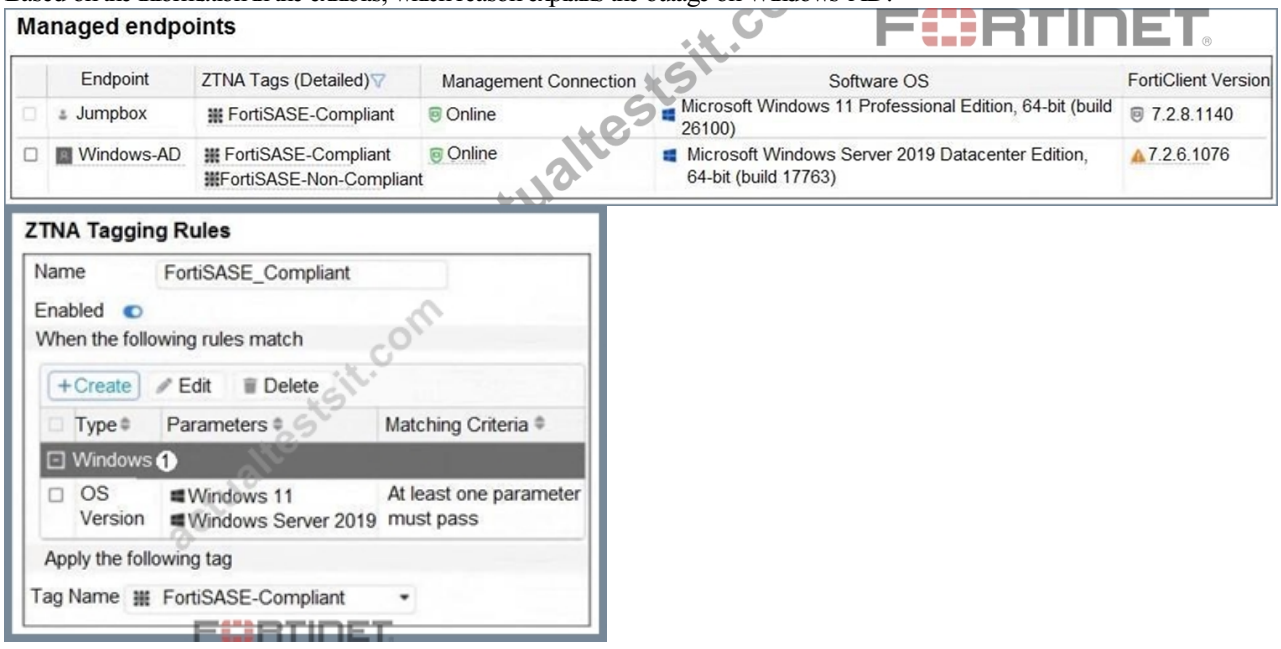
NEW QUESTION # 42
How does FortiSASE Secure Private Access (SPA) facilitate connectivity to private resources in a hub-and- spoke network? (Choose one answer)

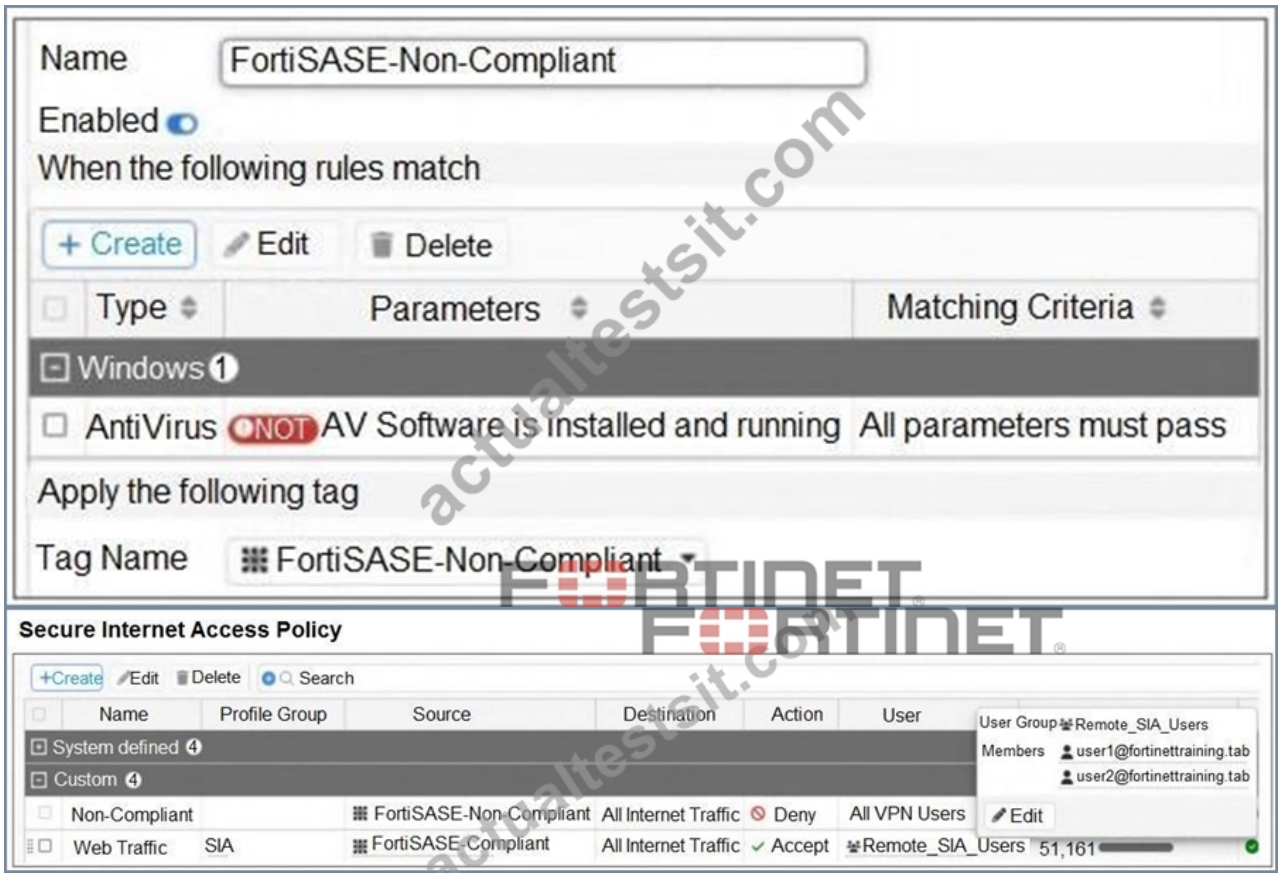
- A. SPA applies source network address translation (SNAT) for remote user traffic and uses IKEv1 for IPsec tunnels to connect to standalone hubs without BGP support.
- B. SPA establishes direct links to spokes without IPsec or BGP and uses an easy configuration key to secure web traffic for remote users.
- C. SPA connects a FortiSASE POP to a FortiGate hub or SD-WAN deployment using IPsec and BGP for dynamic route exchange, with an easy configuration key for simplified setup on FortiOS.
- D. SPA connects to private resources using HTTP and HTTPS protocols and relies on FortiClient for agentless access to SD-WAN deployments.

Answer: C

Explanation:
The correct answer is D . The FortiSASE study guide explains that SPA allows a FortiSASE POP to act as a spoke and connect to a FortiGate hub. It states that you can use FortiSASE SPA so that a POP connects to either a standalone hub using IPsec or to an existing Fortinet SD-WAN deployment . It also states that the BGP protocol is established through IPsec links for dynamic route exchange, which gives FortiSASE remote users access to private resources. For hub deployments running FortiOS 7.4.5 or later, the guide explains that an easy configuration key can simplify SPA setup on FortiSASE by automatically populating key fields in the FortiGate hub configuration.
The wrong options contradict the guide. Option A is false because FortiSASE does not apply SNAT for remote VPN user and edge device traffic destined for SPA hubs, and FortiSASE spokes support IKEv2, not IKEv1. Option B confuses agentless ZTNA with SD-WAN private access. Option C is wrong because SPA uses IPsec and BGP, and the easy configuration key is for SPA hub setup, not for securing general web traffic.

NEW QUESTION # 43
Refer to the exhibits. Jumpbox and Windows-AD are endpoints from the same remote location.
Jumpbox can access the internet through FortiSASE, while Windows-AD can no longer access the internet.
Based on the information in the exhibits, which reason explains the outage on Windows-AD?





- A. The device posture for Windows-AD has changed.
- B. The remote VPN user on Windows-AD no longer matches any VPN policy.
- C. The FortiClient version installed on Windows AD does not match the expected version on FortiSASE.
- D. Windows-AD is excluded from FortiSASE management.

Answer: A

Explanation:
The Windows-AD endpoint now has both "FortiSASE-Compliant" and "FortiSASE-Non- Compliant" tags due to failing the antivirus software check. As a result, the Secure Internet Access Policy matches the "Non-Compliant" rule, which is set to Deny, causing the device to lose internet access.

NEW QUESTION # 44
What are the two key features and benefits of Fortinet SOCaaS when integrated with FortiSASE? (Choose two answers)

- A. Fortinet SOCaaS allows for consistent security monitoring through log forwarding, offers rapid threat notifications and response guidance, and includes intuitive dashboards.
- B. Fortinet SOCaaS monitors only remote users, does not support log forwarding, and provides threat notifications without response guidance or expert meetings.
- C. Fortinet SOCaaS is a standalone service that monitors only FortiGate environments, provides automated patching without human analysis, and does not integrate with FortiSASE.
- D. Fortinet SOCaaS provides 24x7x365 cloud-based monitoring by Fortinet experts using AI, machine learning, and human analysis.
- E. Fortinet SOCaaS offers monitoring only during standard business hours, uses AI without human analysis, and provides annual reports without dashboards or FortiSASE integration.

Answer: A,D

Explanation:
Integrating Fortinet SOCaaS (Security Operations Center as a Service) with FortiSASE provides a managed extension of your security team, combining automated AI/ML-driven triage with human expertise to secure remote and on-premises users.
* Consistent Security Monitoring and Dashboards (C): Fortinet SOCaaS ensures that your security posture remains robust through

seamless integration. This is achieved by configuring FortiSASE to forward pertinent security logs to the SOCaaS cloud, ensuring that analysts have the necessary data to detect anomalies across your network. The service provides verified threat notifications with detailed response guidance and mitigation recommendations. Furthermore, a built-in portal offers intuitive dashboards to track threats and manage escalated alerts.
* 24x7x365 Expert-Led Monitoring (D): This feature addresses the cybersecurity skills gap by providing around-the-clock vigilance. A global team of Fortinet Security Analysts works 24x7x365 to monitor logs and investigate events. The platform leverages AI and Machine Learning for automated alert triage, while human experts perform in-depth analysis to eliminate false positives and validate threats.
* Operational Efficiency: By offloading tedious manual work and triage to Fortinet experts, your internal security team can reduce burnout and focus on higher-value tasks while maintaining a superior security posture for both SASE and on-premises environments.

NEW QUESTION # 45
.....