

# Reliable NSE7\_SSE\_AD-25 Test Sample | Efficient Fortinet NSE7\_SSE\_AD-25 Test Fee: Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator

## STANDARD SEVEN MOCK EXAM

NON SOLVED AND SOLVED

What's more, part of that Dumpleader NSE7\_SSE\_AD-25 dumps now are free: <https://drive.google.com/open?id=1-GbKbvwtO7TZ3XtqJ2-bumD41vhbU19T>

By attempting these Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator (NSE7\_SSE\_AD-25) mock exams, you can enhance your confidence and overcome weaknesses. The NSE7\_SSE\_AD-25 desktop software of Dumpleader works offline on Windows computers. The web-based Fortinet NSE7\_SSE\_AD-25 Practice Exam is compatible with all operating systems and browsers.

### Fortinet NSE7\_SSE\_AD-25 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Analytics: This section covers troubleshooting connectivity and endpoint issues, analyzing dashboards and logs, and reviewing reports related to user traffic and security events.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>Secure Private Access (SPA): This domain includes designing SPA use cases, deploying SPA with SD-WAN, and implementing ZTNA with tagging rules and access proxy configurations.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>SASE deployment and management: This section focuses on deploying and managing FortiSASE for branch and remote users, configuring advanced inspection features, and managing endpoint profiles and compliance rules.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>SASE architecture and integration: This domain covers integrating FortiSASE into existing networks, identifying core SASE components, and evaluating their roles in advanced deployment scenarios.</li></ul>

# Fortinet NSE7\_SSE\_AD-25 Test Fee - NSE7\_SSE\_AD-25 Test Cram Pdf

The updated pattern of Fortinet NSE7\_SSE\_AD-25 Practice Test ensures that customers don't face any real issues while preparing for the test. The students can give unlimited to track the performance of their last given tests in order to see their mistakes and try to avoid them while giving the final test. Customers of Dupleader will receive updates till 1 year after their purchase.

## Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator Sample Questions (Q41-Q46):

### NEW QUESTION # 41

Refer to the exhibit. Which type of information or actions are available to a FortiSASE administrator from the following output?

Name	Vendor	Version	First Detected	Last Installed	Endp
7-Zip 25.00 (x64)	Igor Pavlov	25.00	2025/08/07 03:17:26	2025/07/05	1
Add Folder Suggestions dialog	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
Add Folder Suggestions dialog	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
Adobe Acrobat DC (64-bit)	Adobe	22.001.20117	2025/08/28 11:18:27	2025/05/11	1
Adobe Refresh Manager	Adobe Systems Incorporated	1.8.0	2025/08/28 11:18:27	2025/08/28	1
App Installer	Microsoft Corporation	1.26.430.0	2025/08/20 06:01:00	2025/08/28	1
Application Verifier x64 External Package (DesktopEditions)	Microsoft	10.1.26100.4188	2025/08/07 03:17:26	2025/07/04	1
Application Verifier x64 External Package (OneCoreUAP)	Microsoft	10.1.26100.4188	2025/08/07 03:17:26	2025/07/04	1
Assigned Access Lock app	Microsoft Corporation	1000.19041.4239.0	2025/08/29 11:35:59	2025/08/29	1
AsyncTextService	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
AsyncTextService	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
Captive Portal Flow	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
Captive Portal Flow	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
CapturePicker	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1

- A. Administrators can view and configure endpoint profiles and ZTNA tags.
- B. Administrators can view latest application version available and push updates to managed endpoints.
- C. Administrators can view application details, such as vendor, version, and installation dates to identify unwanted or outdated software.
- D. Administrators can view and configure automatic patching of endpoints, and first detected date for applications.

Answer: C

Explanation:

The software installations page provides detailed information about applications on endpoints, including vendor, version, and installation dates. This allows administrators to identify unwanted or outdated software. It does not allow direct patching, updates, or configuration of endpoint profiles or ZTNA tags from this view.

### NEW QUESTION # 42

A company must provide access to a web server through FortiSASE secure private access for contractors. What is the recommended method to provide access?

- A. Update the DNS records on the endpoint to access private applications.
- B. Update the PAC file with the web server URL and share it with contractors.
- C. Configure a TCP access proxy forwarding rule and push it to the contractor FortiClient endpoint.
- D. Publish the web server URL on a bookmark portal and share it with contractors.

Answer: C

Explanation:

Secure Private Access (SPA) in FortiSASE uses application access rules such as TCP forwarding proxies to securely publish private web applications to external users like contractors.

These rules are pushed to FortiClient endpoints to ensure controlled, identity-based access to the internal web server without exposing it publicly.

### NEW QUESTION # 43

What can be configured on FortiSASE as an additional layer of security for FortiClient registration?

- A. user verification
- **B. device identification**
- C. application inventory
- D. security posture tags

**Answer: B**

Explanation:

Device identification can be configured on FortiSASE as an extra layer of security during FortiClient registration to ensure that only authorized devices can connect to the FortiSASE service.

### NEW QUESTION # 44

How does FortiSASE address the market trends of multicloud and Software-as-a-Service (SaaS) adoption, hybrid workforce, and zero trust? (Choose one answer)

- A. It prioritizes legacy VPN connections for hybrid workforces, bypassing modern cloud and zero-trust security measures.
- **B. It provides visibility and control for multicloud and SaaS environments, ensures secure and seamless access for hybrid workforces, and implements zero-trust principles.**<sup>1</sup>
- C. It focuses solely on securing on-premises networks, ignoring cloud and remote work challenges.
- D. It supports only zero-trust frameworks without addressing multicloud or hybrid workforce needs.

**Answer: B**

Explanation:

FortiSASE is designed as a unified, single-vendor solution that specifically targets the convergence of networking and security to address the modern challenges of a distributed enterprise.<sup>2</sup>

\* Multicloud and SaaS Adoption: FortiSASE addresses the surge in cloud-first strategies by providing Next-Generation Dual-Mode CASB (Cloud Access Security Broker).<sup>3</sup> This feature uses both inline and API-based inspection to provide comprehensive visibility into sanctioned and unsanctioned SaaS applications (Shadow IT), ensuring that data is protected regardless of whether it resides in AWS, Azure, Google Cloud, or SaaS platforms like Microsoft 365.

\* Hybrid Workforce: To support a workforce that moves between the home, the office, and public spaces, FortiSASE delivers consistent security posture.<sup>5</sup> It replaces the inconsistent experience of legacy VPNs with a geographically dispersed network of over 150 Points of Presence (PoPs), ensuring low-latency access to applications while maintaining high-performance SSL inspection and threat detection for all remote users.

\* Zero Trust Integration: Central to the FortiSASE architecture is Universal ZTNA (Zero Trust Network Access).<sup>7</sup> Unlike traditional VPNs that grant broad network access, ZTNA applies the principle of "never trust, always verify". It grants access on a per-session, per-application basis, continuously verifying the device posture and user identity before and during application access.<sup>9</sup> This shift from implicit to explicit trust significantly reduces the internal attack surface and mitigates the risk of lateral movement by attackers.

By integrating these components into a single operating system (FortiOS) and managed via a single console, FortiSASE simplifies IT operations while delivering the visibility and control required for today's multicloud and hybrid environments.

### NEW QUESTION # 45

Refer to the exhibits.

Endpoint	ZTNA Tags (Detailed)	Management Connection	Software OS	FortiClient Version
Jumpbox	FortiSASE-Compliant	Online	Microsoft Windows 11 Professional Edition, 64-bit (build 26100)	7.2.8.1140
Windows-AD	FortiSASE-Compliant FortiSASE-Non-Compliant	Online	Microsoft Windows Server 2019 Datacenter Edition, 64-bit (build 17763)	7.2.6.1076

ZTNA Tagging Rules

Name: FortiSASE\_Compliant

Enabled:

When the following rules match

- Windows (1)
- OS Version: Windows 11, Windows Server 2019. Matching Criteria: At least one parameter must pass.

Apply the following tag

Tag Name: FortiSASE-Compliant

Secure Internet Access Policy

Name	Profile Group	Source	Destination	Action	User
Non-Compliant	SIA	FortiSASE-Non-Compliant	All Internet Traffic	Deny	All VPN Users
Web Traffic	SIA	FortiSASE-Compliant	All Internet Traffic	Accept	Remote_SIA_Users

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? (Choose one answer)

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

Answer: A

Explanation:

In FortiSASE, Zero Trust Network Access (ZTNA) tags-also known as security posture tags-are used to dynamically grant or deny access based on the real-time security state of an endpoint. This mechanism ensures that only devices meeting specific compliance requirements can access protected resources or the internet.

\* Endpoint Analysis: The Managed Endpoints exhibit shows that while Jumpbox only has the FortiSASE-Compliant tag, the Windows-AD endpoint has been assigned both FortiSASE-Compliant and FortiSASE-Non-Compliant tags. This indicates that a security posture check on the Windows-AD device has failed, triggering a rule that applies the non-compliant tag.

\* Policy Evaluation: The Secure Internet Access Policy table shows two custom policies. The first policy, named Non-compliant, uses the FortiSASE-Non-Compliant tag as its source and has the action set to Deny. The second policy, Web Traffic, allows access for FortiSASE-Compliant users.

\* Root Cause of Outage: Because FortiSASE (powered by FortiOS) processes security policies in a top- down sequence, the "Non-compliant" policy is evaluated first. Since Windows-AD matches the source criteria for this "Deny" policy, its traffic is blocked before it can reach the "Accept" policy.

Although the exhibit shows a warning icon for the FortiClient version on Windows-AD, the direct cause of the internet outage is the explicit Deny policy triggered by the change in the device's security posture (the application of the Non-Compliant tag).

NEW QUESTION # 46

.....

Do you often feel that your ability does not match your ambition? Are you dissatisfied with the ordinary and boring position? If your answer is yes, you can try to get the NSE7\_SSE\_AD-25 certification that you will find there are so many chances wait for you. You

