

# Free Download FCSS\_SASE\_AD-24 Latest Exam Testking & Guaranteed Fortinet FCSS\_SASE\_AD-24 Exam Success with Perfect FCSS\_SASE\_AD-24 Exam Consultant

FORTINET



P.S. Free & New FCSS\_SASE\_AD-24 dumps are available on Google Drive shared by TestPassKing: <https://drive.google.com/open?id=1vx27tkcwAoRShNV-Iw9rPOIwwUotS4zS>

As a top selling product in the market, our FCSS\_SASE\_AD-24 study materials have many fans. They are keen to try our newest version products even if they have passed the FCSS\_SASE\_AD-24 exam. They never give up learning new things. Every time they try our new version of the FCSS\_SASE\_AD-24 Study Materials, they will write down their feelings and guidance. Also, they will exchange ideas with other customers. They give our FCSS\_SASE\_AD-24 study materials strong support. So we are deeply moved by their persistence and trust.

Actually, one of the most obvious advantages of our FCSS\_SASE\_AD-24 simulating questions is their profession, which is realized by the help from our experts. We invited a large group of professional experts who dedicated in this area for more than ten years. To improve the accuracy of the FCSS\_SASE\_AD-24 Guide preparations, they keep up with the trend closely. Every page of our FCSS\_SASE\_AD-24 practice engine is carefully arranged by them with high efficiency and high quality.

>> FCSS\_SASE\_AD-24 Latest Exam Testking <<

## FCSS\_SASE\_AD-24 Exam Consultant | FCSS\_SASE\_AD-24 Reliable Test Dumps

Our Fortinet FCSS\_SASE\_AD-24 Exam Dumps effect in helping candidates' certification exam. Original questions are also important. These would provide a forum where certification training can be carried on. Our dumps torrent is perfect and practice test is also the latest. After you purchase our product, we offer free update service for one year.

### Fortinet FCSS\_SASE\_AD-24 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>SASE Architecture and Components: This section measures the skills of Network Security Engineers and covers the architecture and components of FortiSASE. It includes integrating FortiSASE into a hybrid network, identifying its components, and constructing deployment cases to effectively implement SASE solutions.</li></ul>

Topic 2	<ul style="list-style-type: none"> <li>• SIA, SSA, and SPA" This section focuses on the skills of Security Administrators in designing security profiles for content inspection and deploying SD-WAN and Zero Trust Network Access (ZTNA) using SASE. Understanding these concepts is crucial for securing access to applications and data across the network.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• SASE Deployment: This domain assesses the capabilities of Cloud Security Architects in deploying SASE solutions. It includes implementing various user onboarding methods, configuring administration settings, and applying security posture checks and compliance rules to ensure a secure environment.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• Analytics: This domain evaluates the skills of Data Analysts in utilizing analytics within FortiSASE. It involves identifying potential security threats using traffic logs, configuring dashboards and logging settings, and analyzing reports for user traffic and security issues to enhance overall security posture.</li> </ul>

## Fortinet FCSS - FortiSASE 24 Administrator Sample Questions (Q11-Q16):

### NEW QUESTION # 11

What are two requirements to enable the MSSP feature on FortiSASE? (Choose two.)

- A. Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal.
- B. Enable multi-tenancy on the FortiSASE portal.
- C. Add FortiCloud premium subscription on the root FortiCloud account.
- D. Configure MSSP user accounts and permissions on the FortiSASE portal.

**Answer: A,B**

Explanation:

To enable the MSSP (Managed Security Service Provider) feature on FortiSASE, two key requirements must be met:

Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal (Option C):

RBAC is essential for managing permissions and ensuring that different customers (tenants) have appropriate access levels. The FortiCloud Identity and Access Management (IAM) portal allows administrators to define roles and assign them to users, ensuring secure and granular control over resources.

Enable multi-tenancy on the FortiSASE portal (Option D):

Multi-tenancy is a critical feature for MSSPs, as it allows them to manage multiple customer environments (tenants) from a single FortiSASE instance. Each tenant operates independently with its own configurations, policies, and reporting, while the MSSP retains centralized control.

Here's why the other options are incorrect:

A . Add FortiCloud premium subscription on the root FortiCloud account: While FortiCloud subscriptions may enhance functionality, they are not specifically required to enable the MSSP feature.

B . Configure MSSP user accounts and permissions on the FortiSASE portal: User accounts and permissions are managed through the FortiCloud IAM portal, not directly on the FortiSASE portal.

Reference:

Fortinet FCSS FortiSASE Documentation - MSSP Feature Configuration

FortiSASE Administration Guide - Multi-Tenancy and RBAC Setup

### NEW QUESTION # 12

Which two statements describe a zero trust network access (ZTNA) private access use case? (Choose two.)

- A. All TCP-based applications are supported.
- B. Data center redundancy is offered.
- C. The security posture of the device is secure.
- D. All FortiSASE user-based deployments are supported.

**Answer: A,C**

Explanation:

Zero Trust Network Access (ZTNA) private access use cases focus on providing secure and controlled access to private applications without exposing them to the public internet. The following two statements accurately describe ZTNA private access use cases:

\* The security posture of the device is secure (Option A):ZTNA enforces strict access controls based on the principle of least privilege. Before granting access to private applications, ZTNA evaluates the security posture of the device (e.g., whether it is patched, compliant, and free of malware). Only devices that meet the required security standards are granted access, ensuring that the device is secure before allowing private access.

\* All TCP-based applications are supported (Option C):ZTNA supports all TCP-based applications, enabling secure access to a wide range of private applications, including legacy systems and custom- built applications. This flexibility makes ZTNA suitable for organizations with diverse application environments.

Here's why the other options are incorrect:

\* B. All FortiSASE user-based deployments are supported:While FortiSASE supports various deployment scenarios, not all user-based deployments are automatically compatible with ZTNA.

Specific configurations and requirements must be met to enable ZTNA functionality.

\* D. Data center redundancy is offered:Data center redundancy is unrelated to ZTNA private access use cases. Redundancy typically pertains to infrastructure design and failover mechanisms, not access control methodologies like ZTNA.

References:

Fortinet FCSS FortiSASE Documentation - ZTNA Private Access Overview

FortiSASE Administration Guide - ZTNA Deployment Best Practices

### NEW QUESTION # 13

What aspects should be considered when designing security profiles for content inspection?

(Choose Two)

Response:

- A. Data throughput rates
- B. Encryption standards used in data transfer
- C. Types of data to be inspected
- D. User authentication protocols

**Answer: B,C**

### NEW QUESTION # 14

Refer to the exhibit.

To allow access, which web filter configuration must you change on FortiSASE?

- A. FortiGuard category-based filter
- B. URL Filter
- C. inline cloud access security broker (CASB) headers
- D. content filter

**Answer: D**

### NEW QUESTION # 15

Refer to the exhibits.

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The VPN tunnel does not establish. Based on the provided configuration, what configuration needs to be modified to bring the tunnel up?

- A. The BGP router ID needs to match on the hub and FortiSASE.
- B. The hub needs IKEv2 enabled in the IPsec phase 1 settings.
- C. FortiSASE spoke devices do not support mode config.
- D. NAT needs to be enabled in the Spoke-to-Hub firewall policy.

**Answer: B**

### NEW QUESTION # 16

.....

