

Boost up Your Certification Score

Fortinet

FCSS_SASE_AD-24

Fortinet FCSS - FortiSASE 24 Administrator



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which VDOM type needs to be configured on the FortiGate Secure Edge to establish a layer 2 network between itself and FortiSASE?

Response:

- A. Transparent
- B. Traffic
- C. Admin
- D. LAN-Extension

Answer: D

Question: 2

When using Secure Private Access (SPA) and SD-WAN, which protocol is used for spoke-to-spoke connectivity?

Response:

- A. eBGP
- B. SSL
- C. IPSEC
- D. GRE

Answer: C

Question: 3

Which FortiSASE Secure Private Access (SPA) deployment involves installing FortiClient on remote endpoints?

Response:

- A. MicroBranch
- B. zero trust network access (ZTNA)
- C. secure web gateway (SWG)
- D. SD-WAN

Answer: B

Question: 4

How does integrating endpoint detection and response (EDR) systems into SASE contribute to security posture?

Response:

- A. It isolates the network from the internet
- B. It provides real-time threat detection and response at endpoints
- C. It serves as the primary firewall
- D. It enhances user interface designs

Answer: B

Question: 5

Which dedicated IP address use case allows application of SNAT to specific incoming remote users based on user, group, or country?

Response:

- A. Identification and isolation
- B. Source IP anchoring
- C. Central SNAT policy
- D. Geolocation rules

Answer: B

Question: 6

Which FortiSASE component can be utilized for endpoint compliance?

Response:

- A. Firewall-as-a-Service (FWaaS)
- B. zero trust network access (ZTNA)
- C. cloud access security broker (CASB)
- D. secure web gateway (SWG)

Answer: B

Question: 7

Which three ways does FortiSASE provide Secure Private Access (SPA) to corporate, non-web applications?

(Choose three.)

Response:

- A. Using SD-WAN technology
- B. Using secure web gateway (SWG)
- C. Using zero trust network access (ZTNA) technology
- D. Using digital experience monitoring
- E. Using next generation firewall (NGFW)

Answer: A,C,E

Question: 8

Which endpoint functionality can you configure using FortiSASE?

Response:

- A. You can configure inline sandbox to scan zero-day malware attacks.
- B. You can enable and push web filter to FortiClient endpoints.
- C. It can be applied to both SWG and VPN deployments.
- D. Site-based FortiExtender users can perform on-demand vulnerability scans.

Answer: A

Question: 9

Which FortiSASE feature can you use to see a list of Software-as-a-Service (SaaS) applications and health-check metrics for first-mile connectivity between the geographical points of presence (PoPs) provisioned for your FortiSASE instance and these SaaS applications?

Response:

- A. event logs
- B. digital experience monitoring DEM
- C. FortiView
- D. security logs

Answer: B

Question: 10

Which feature can assist FortiSASE administrators with troubleshooting remote user connectivity issues to common SaaS applications using health check metrics?

Response:

- A. Security logs
- B. Event logs
- C. FortiView Dashboards
- D. Digital Experience Monitoring

Answer: D

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/fcss-sase-ad-24>