DUMPSBOSS.

FCSSFortiSASE 24 Administrator

Fortinet FCSS_SASE_AD-24

Version Demo

Total Demo Questions: 7

Total Premium Questions: 72

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSASE Deployment	17
Topic 2, Secure Internet Access	14
Topic 3, Secure Private Access	16
Topic 4, SaaS Security	7
Topic 5, Endpoint Security	8
Topic 6, Monitoring and Operations	10
Total	72

QUESTION NO: 1

An organization wants noncompliant endpoints to be denied access to a private application, while compliant endpoints continue to have access.

Which two statements describe the FortiSASE posture-based access workflow? (Choose two.)

A. FortiClient telemetry can evaluate the endpoint security conditions.

B. A private access policy can match the endpoint compliance-related ZTNA tag.

C. A failed posture check automatically disconnects FortiClient telemetry.

D. A failed posture check automatically blocks all endpoint network access.

ANSWER: A B

Explanation:

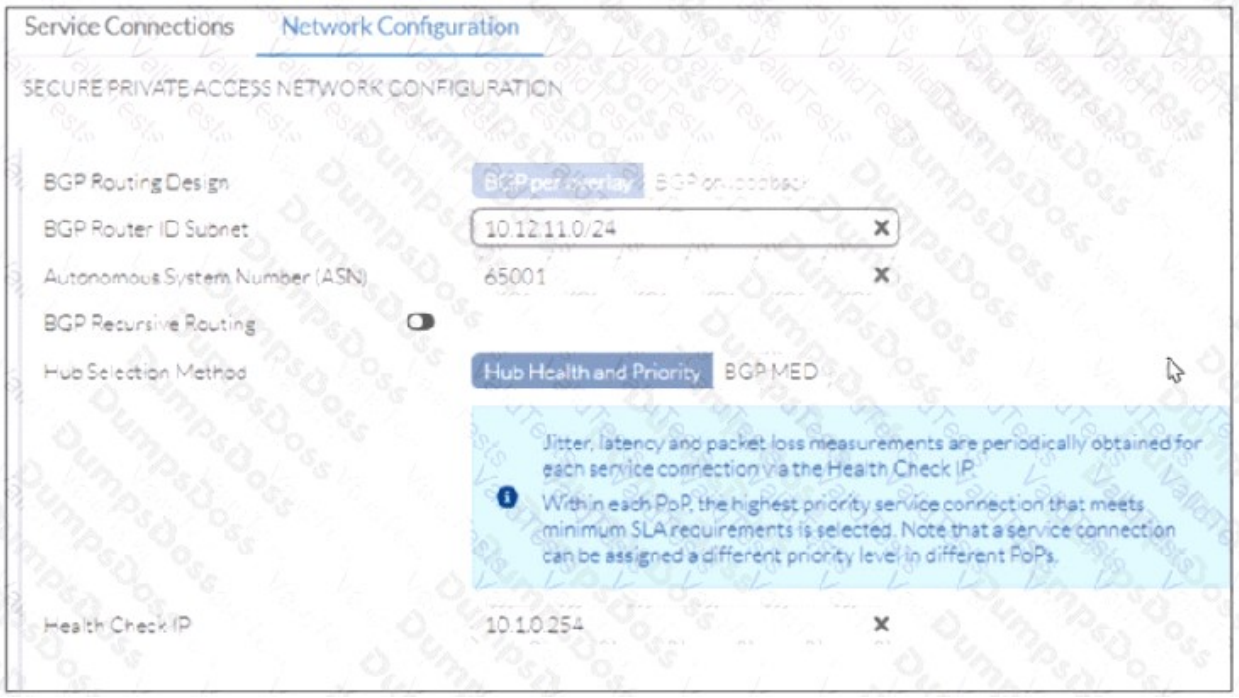
FortiClient telemetry is used to evaluate endpoint security conditions, and FortiSASE can classify the endpoint with a compliance-related ZTNA tag. A private access policy can then match the appropriate tag to grant or deny access to the protected application.

A failed posture evaluation does not automatically disconnect all FortiClient telemetry or universally block network access. The resulting access decision depends on the configured policy that matches the endpoint tag.

QUESTION NO: 2

Refer to the exhibits.

Secure private access network connection



Firewall policy configuration

```
config firewall policy
    edit 5
        set name "Spoke-to-Spoke"
        set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
        set srcintf "To_SASE"
        set dstintf "To_SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
    edit 6
        set name "Lo-BGP-HC"
        set uuid f5a12c92-216b-51ee-4802-80cd013d6acf
        set srcintf "To_SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
    edit 9
        set name "Spoke-to-Hub"
        set uuid 617b81ee-cc64-51ee-8da6-6cdff3ca2cca
        set dstintf "internal3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

IPsec VPN configuration

```
# show vpn ipsec phase1-interface To_SASE
 config vpn ipsec phase1-interface
    edit "To_SASE"
        set type dynamic
        set interface "wan1"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: To_SASE (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable
        set ipv4-start-ip 10.11.11.10
        set ipv4-end-ip 10.11.11.200
        set ipv4-netmask 255.255.255.0
        set unity-support disable
        set psksecret ENC SblOigpvIFFYSpRZ/hyxQVUXv9NZm7uqltD9v+BViPd+7RWizmUA3ZINn0zbsxq70F
  iYkPLkxaNwIo7VLIipkye1xt84NAwEfm5jTqqf1dMj/phYvBI3hzU0yXg==
    next
 end

# show vpn ipsec phase2-interface To_SASE
config vpn ipsec phase2-interface
    edit "To_SASE"
        set phase1name "To_SASE"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
 end
```

BGP protocol configuration

```
#config router bgp
     set as 65001
     set router-id 10.1.0.254
     config neighbor
         edit "10.10.1.3"
             set advertisement-interval 1
             set ebgp-enforce-multihop enable
             set link-down-failover enable
             set remote-as 65001
             set route-reflector-client enable
         next
     end
     config neighbor-group
         edit "To_SASE"
             set capability-graceful-restart enable
             set link-down-failover enable
             set next-hop-self enable
             set interface "To_SASE"
             set remote-as 65001
             set additional-path both
             set adv-additional-path 4
             set route-reflector-client enable
         next
     end
     config neighbor-range
         edit 1
             set prefix 10.11.11.0 255.255.255.0
             set neighbor-group "To_SASE"
         next
     end
     config network
         edit 1
             set prefix 10.190.190.0 255.255.255.0
         next
     end
```

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. NAT needs to be enabled in the Spoke-to-Hub firewall policy.

B. The BGP router ID needs to match on the hub and FortiSASE.

C. FortiSASE spoke devices do not support mode config.

D. The hub needs IKEv2 enabled in the IPsec phase 1 settings.

ANSWER: D

Explanation:

The hub needs IKEv2 enabled in the IPsec phase 1 settings. FortiSASE uses IKEv2 for IPsec VPN connectivity when it is configured as a spoke to a FortiGate hub. IKE negotiation is performed before phase 2 selectors, routing, and traffic policies can be evaluated. Therefore, the FortiGate hub's phase 1 configuration must use an IKE version compatible with the FortiSASE spoke. If the hub is configured only for IKEv1, the peers cannot complete the initial security-association negotiation, so no IPsec tunnel is established.

Enable IKEv2 on the relevant FortiGate IPsec phase 1 interface and ensure that the remaining phase 1 parameters shared by the peers, such as the remote gateway information, authentication method, pre-shared key or certificate configuration,

and cryptographic proposals, remain aligned. Once IKEv2 is enabled and the common phase 1 settings match, the hub and FortiSASE can negotiate the IKE security association and bring up the tunnel. Fortinet's FortiSASE documentation is available through the FortiSASE documentation portal, and FortiGate IPsec configuration guidance is available in the FortiGate IPsec VPN documentation.

QUESTION NO: 3

A FortiSASE administrator is configuring a Secure Private Access (SPA) solution to share endpoint information with a corporate FortiGate.

Which three configuration actions will achieve this solution? (Choose three.)

A. Add the FortiGate IP address in the secure private access configuration on FortiSASE.

B. Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE

C. Register FortiGate and FortiSASE under the same FortiCloud account.

D. Authorize the corporate FortiGate on FortiSASE as a ZTNA access proxy.

E. Apply the FortiSASE zero trust network access (ZTNA) license on the corporate FortiGate.

ANSWER: B C D

Explanation:

Secure Private Access integrates FortiSASE-managed endpoint context with an on-premises FortiGate so that the FortiGate can use endpoint-related information when providing protected access to private resources. The FortiGate must use the FortiClient EMS cloud connector to establish its association with the FortiSASE service; this is the integration mechanism that lets the FortiGate obtain the relevant endpoint and telemetry context from the Fortinet cloud service. FortiGate and FortiSASE must also be registered to the same FortiCloud account. This common account establishes the required ownership and authorization relationship, allowing the FortiSASE tenant and the FortiGate appliance to be associated securely. Finally, the FortiGate must be authorized in FortiSASE as a ZTNA access proxy. That authorization identifies the corporate FortiGate as the approved enforcement and access-proxy device for the SPA deployment, enabling it to participate in the ZTNA workflow using the shared endpoint information. These steps collectively establish cloud identity association, connector-based endpoint-context sharing, and access-proxy authorization. Fortinet's FortiSASE documentation and FortiGate documentation provide the product configuration references for this integration.

QUESTION NO: 4

An organization has previously configured local user authentication for FortiSASE. The administrator then enables single sign-on (SSO) with the organization's identity provider.

How will FortiSASE authenticate users after SSO is enabled?

A. It authenticates users through the configured identity provider instead of the previous user authentication.

B. It authenticates users through local authentication before redirecting them to the identity provider.

C. It uses SSO only when a FortiClient endpoint cannot authenticate locally.

D. It uses SSO only for users connecting through an agent-based deployment.

ANSWER: A

Explanation:

SSO overrides previously configured user authentication. FortiSASE redirects users to the configured identity provider and uses the resulting SAML authentication assertion to establish the user identity.

Local authentication is not evaluated first as a fallback authentication method for the SSO deployment. SSO is also not limited to agent-based users; it is an identity-provider-based authentication workflow for the applicable FortiSASE access deployment.

QUESTION NO: 5

Which two advantages does FortiSASE bring to businesses with multiple branch offices? (Choose two.)

A. It offers centralized management for simplified administration.

B. It enables seamless integration with third-party firewalls.

C. it offers customizable dashboard views for each branch location

D. It eliminates the need to have an on-premises firewall for each branch.

ANSWER: A D

Explanation:

FortiSASE offers centralized management for simplified administration because it delivers security and access controls through a unified, cloud-managed platform. For organizations operating many branches, administrators can consistently configure and administer security services, policies, users, and connectivity without having to manage each location as an entirely separate security environment. This helps reduce operational overhead while supporting consistent policy enforcement across distributed offices.

FortiSASE also eliminates the need to have an on-premises firewall for each branch when the branch's security requirements can be delivered through the FortiSASE cloud service rather than by dedicated firewall hardware at every site. Internet-bound traffic and access to cloud applications can be protected with cloud-delivered security capabilities, which can lower branch hardware requirements and simplify deployment for suitable branch designs. Together, centralized cloud administration and cloud-delivered security make FortiSASE particularly useful for organizations seeking to standardize and streamline security across multiple locations.

Fortinet describes FortiSASE as a cloud-delivered SASE solution that converges networking and security services: Fortinet FortiSASE. FortiSASE administration documentation is available at FortiSASE Documentation.

QUESTION NO: 6

A remote endpoint uses a split DNS rule for the internal domain corp.example. Queries for internal hostnames are sent to the internal DNS servers, but they time out while the endpoint is connected to FortiSASE.

Which configuration is most likely missing?

A. Add the internal DNS server addresses to split tunnelling destinations.

B. Enable SSL deep inspection for DNS traffic.

C. Apply a DNS filter profile to the secure web gateway policy.

D. Create a web filter exception for the internal domain.

ANSWER: A

Explanation:

The internal DNS server addresses must be reachable through the FortiSASE private access path. Split DNS rules determine which DNS suffixes use internal resolvers, but split tunnelling destinations provide the required path to reach those private DNS servers.

SSL deep inspection and DNS filtering do not create connectivity to an internal DNS server. A web filter profile is unrelated to private DNS resolution.

QUESTION NO: 7

Which event log subtype captures FortiSASE SSL VPN user creation?

A. Endpoint Events

B. VPN Events

C. User Events

D. Administrator Events

ANSWER: C

Explanation:

User Events is the appropriate event-log subtype because creating an SSL VPN user is a user-lifecycle and identity-management action. FortiSASE records operations that add, modify, or remove user identities in the user-focused event category, allowing administrators to audit when access-capable user accounts are created and to correlate that activity with the administrator or workflow that performed it. This distinction is important for access governance: the significant audited action is the creation of the user identity that can subsequently be granted SSL VPN access, rather than a later connection made by that user. Reviewing User Events therefore provides the audit trail needed to confirm the account-creation operation, investigate changes to the user population, and support administrative accountability. FortiSASE documentation is available through the FortiSASE Documentation Library, which includes administration and logging guidance. For broader product context on FortiSASE secure access and user connectivity, see the FortiSASE product page.