Vendor: Fortinet

Exam Code: FCSS_SASE_AD-24

Exam Name: FCSS - FortiSASE 24 Administrator

Version: DEMO

QUESTION 1
Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles?

A. It offers hardware-based firewalls for network segmentation.
B. It integrates with software-defined network (SDN) solutions.
C. It can identify attributes on the endpoint for security posture check.
D. It enables VPN connections for remote employees.

Answer: C
Explanation:
FortiSASE supports zero trust network access (ZTNA) principles by identifying attributes on the endpoint for security posture checks. ZTNA principles require continuous verification of user and device credentials, as well as their security posture, before granting access to network resources.
Security Posture Check:
FortiSASE can evaluate the security posture of endpoints by checking for compliance with security policies, such as antivirus status, patch levels, and configuration settings. This ensures that only compliant and secure devices are granted access to the network.
Zero Trust Network Access (ZTNA):
ZTNA is based on the principle of "never trust, always verify," which requires continuous assessment of user and device trustworthiness.
FortiSASE plays a crucial role in implementing ZTNA by performing these security posture checks and enforcing access control policies.

QUESTION 2
When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)

A. Vulnerability scan
B. SSL inspection
C. Anti-ransomware protection
D. Web filter
E. ZTNA tags

Answer: ACE

QUESTION 3
Which FortiSASE feature ensures least-privileged user access to all applications?

A. secure web gateway (SWG)
B. SD-WAN
C. zero trust network access (ZTNA)
D. thin branch SASE extension

Answer: C
Explanation:
Zero Trust Network Access (ZTNA) is the FortiSASE feature that ensures least-privileged user access to all applications. ZTNA operates on the principle of "never trust, always verify," providing secure access based on the identity of users and devices, regardless of their location.
Zero Trust Network Access (ZTNA):
ZTNA ensures that only authenticated and authorized users and devices can access applications. It applies the principle of least privilege by granting access only to the resources required by the

---

user, minimizing the potential for unauthorized access.
Implementation:
ZTNA continuously verifies user and device trustworthiness and enforces granular access control policies.
This approach enhances security by reducing the attack surface and limiting lateral movement within the network.

QUESTION 4
Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

A. FortiSASE CA certificate
B. proxy auto-configuration (PAC) file
C. FortiSASE invitation code
D. FortiClient installer

Answer: AB
Explanation:
Onboarding a Secure Web Gateway (SWG) endpoint involves several components to ensure secure and effective integration with FortiSASE. Two key components are the FortiSASE CA certificate and the proxy auto-configuration (PAC) file.
FortiSASE CA Certificate:
The FortiSASE CA certificate is essential for establishing trust between the endpoint and the FortiSASE infrastructure.
It ensures that the endpoint can securely communicate with FortiSASE services and inspect SSL/TLS traffic.
Proxy Auto-Configuration (PAC) File:
The PAC file is used to configure the endpoint to direct web traffic through the FortiSASE proxy. It provides instructions on how to route traffic, ensuring that all web requests are properly inspected and filtered by FortiSASE.

QUESTION 5
To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

A. SD-WAN private access
B. inline-CASB
C. zero trust network access (ZTNA) private access
D. next generation firewall (NGFW)

Answer: C
Explanation:
ZTNA ensures that remote users can securely connect to private applications based on identity verification and security policies, without needing a traditional VPN. This access method provides strong security with least-privilege access, which is ideal for protecting private web servers and their data from unauthorized access. It also improves efficiency by dynamically verifying user identity and device posture before granting access.

QUESTION 6
Which secure internet access (SIA) use case minimizes individual workstation or device setup,

because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based end points?

A. SIA for inline-CASB users
B. SIA for agentless remote users
C. SIA for SSLVPN remote users
D. SIA for site-based remote users

Answer: D
Explanation:
In this use case, secure internet access (SIA) is configured at the site level rather than on individual devices. This approach eliminates the need for individual endpoint setup, such as installing FortiClient or configuring web proxy settings on each workstation or device. It allows centralized management and secure internet access for all users at the site level, simplifying deployment and maintenance.

QUESTION 7
When accessing the FortiSASE portal for the first time, an administrator must select data center locations for which three FortiSASE components? (Choose three.)

A. Endpoint management
B. Points of presence
C. SD-WAN hub
D. Logging
E. Authentication

Answer: ABD
Explanation:
When accessing the FortiSASE portal for the first time, an administrator must select data center locations for the following FortiSASE components:
Endpoint Management:
The data center location for endpoint management ensures that endpoint data and policies are managed and stored within the chosen geographical region.
Points of Presence (PoPs):
Points of Presence (PoPs) are the locations where FortiSASE services are delivered to users. Selecting PoP locations ensures optimal performance and connectivity for users based on their geographical distribution.
Logging:
The data center location for logging determines where log data is stored and managed. This is crucial for compliance and regulatory requirements, as well as for efficient log analysis and reporting.
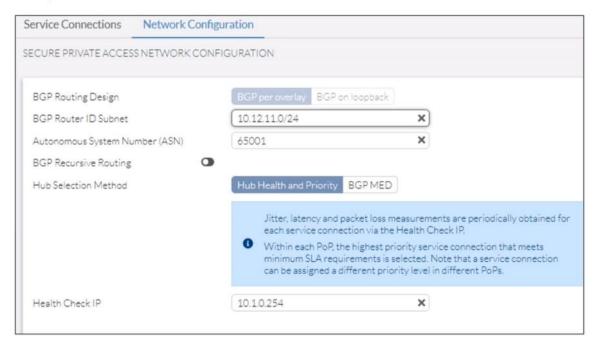
QUESTION 8
Refer to the exhibits. A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The VPN tunnel does not establish.
Based on the provided configuration, what configuration needs to be modified to bring the tunnel up?

Secure private access service connection

UPDATE SECURE PRIVATE ACCESS SERVICE CONNECTION

Name	To_FortiGate ✕
Remote Gateway	203.221.196.6 ✕
Authentication Method	Pre-shared Key Certificate
BGP Peer IP	10.11.11.1 ✕
Network Overlay ID	100 ✕

Secure private access network connection

Service Connections   Network Configuration

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design	BGP per overlay BGP on loopback
BGP Router ID Subnet	10.12.11.0/24 ✕
Autonomous System Number (ASN)	65001 ✕
BGP Recursive Routing	⬤
Hub Selection Method	Hub Health and Priority BGP MED

ℹ Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

Health Check IP	10.1.0.254 ✕

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 srcintf "To_SASE"
        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/phYvBI3hzU0yXq==
    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. 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

QUESTION 9
Which two additional components does FortiSASE use for application control to act as an inline-CASB? (Choose two.)

A. intrusion prevention system (IPS)
B. SSL deep inspection
C. DNS filter
D. Web filter with inline-CASB

Answer: AB
Explanation:
IPS protocol decode and analyze network trafficto detect application traffic.
SSL deep inspection to control SaaS cloud application.

QUESTION 10
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: AD
Explanation:
FortiSASE brings the following advantages to businesses with multiple branch offices:
Centralized Management for Simplified Administration:
FortiSASE provides a centralized management platform that allows administrators to manage
security policies, configurations, and monitoring from a single interface. This simplifies the
administration and reduces the complexity of managing multiple branch offices.
Eliminates the Need for On-Premises Firewalls:
FortiSASE enables secure access to the internet and cloud applications without requiring
dedicated on-premises firewalls at each branch office.
This reduces hardware costs and simplifies network architecture, as security functions are
handled by the cloud-based FortiSASE solution.

QUESTION 11
During FortiSASE provisioning, how many security points of presence (POPs) need to be
configured by the FortiSASE administrator?

A. 3
B. 4
C. 2
D. 1

Answer: D
Explanation:
During FortiSASE provisioning, the FortiSASE administrator needs to configure at least one
security point of presence (PoP). A single PoP is sufficient to get started with FortiSASE,
providing the necessary security services and connectivity for users.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14