Number: FCSS_SASE_AD-23
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: FCSS_SASE_AD-23

Exam Name: FCSS - FortiSASE 23 Administrator

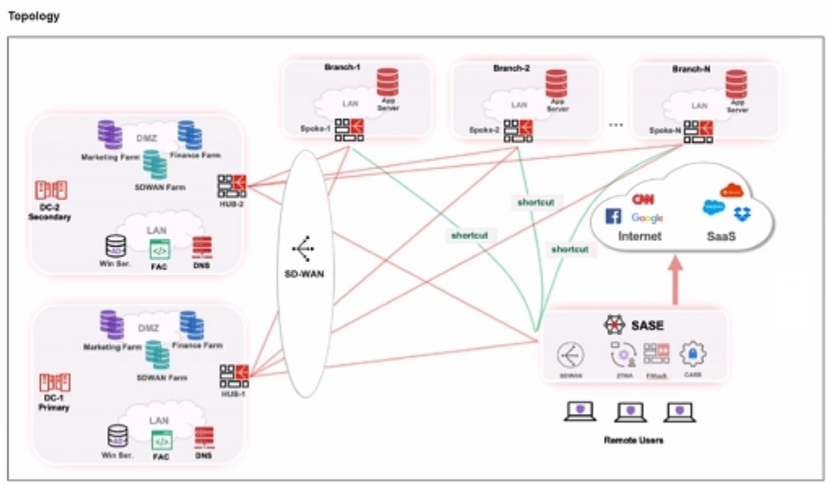
Exam A

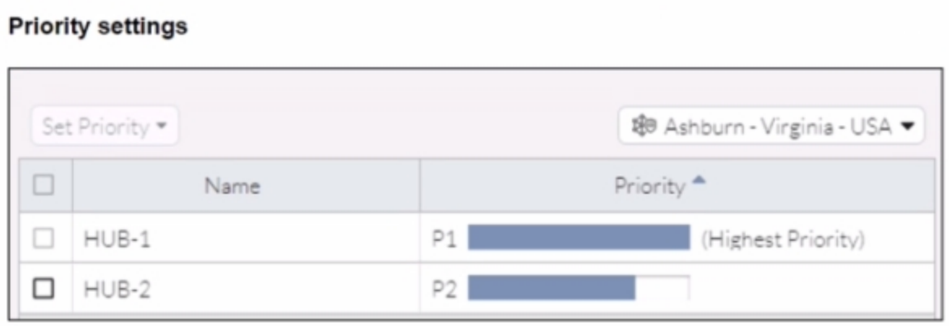
QUESTION 1
Which two deployment methods are used to connect a FortiExtender as a FortiSASE LAN extension? (Choose two.)

A. Connect FortiExtender to FortiSASE using FortiZTP
B. Enable Control and Provisioning Wireless Access Points (CAPWAP) access on the FortiSASE portal.
C. Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server
D. Configure an IPsec tunnel on FortiSASE to connect to FortiExtender.

Correct Answer: A, C
Section:
Explanation:
There are two deployment methods used to connect a FortiExtender as a FortiSASE LAN extension:
Connect FortiExtender to FortiSASE using FortiZTP:
FortiZero Touch Provisioning (FortiZTP) simplifies the deployment process by allowing FortiExtender to automatically connect and configure itself with FortiSASE.
This method requires minimal manual configuration, making it efficient for large-scale deployments.
Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server:
Manually configuring the FortiSASE domain name in the FortiExtender GUI allows the extender to discover and connect to the FortiSASE infrastructure.
This static discovery method ensures that FortiExtender can establish a connection with FortiSASE using the provided domain name.
FortiOS 7.2 Administration Guide: Details on FortiExtender deployment methods and configurations.
FortiSASE 23.2 Documentation: Explains how to connect and configure FortiExtender with FortiSASE using FortiZTP and static discovery.

QUESTION 2
Refer to the exhibits.





When remote users connected to FortiSASE require access to internal resources on Branch-2. how will traffic be routed?

A. FortiSASE will use the SD-WAN capability and determine that traffic will be directed to HUB-2. which will then route traffic to Branch-2.
B. FortiSASE will use the AD VPN protocol and determine that traffic will be directed to Branch-2 directly, using a static route
C. FortiSASE will use the SD-WAN capability and determine that traffic will be directed to HUB-1, which will then route traffic to Branch-2.
D. FortiSASE will use the AD VPN protocol and determine that traffic will be directed to Branch-2 directly, using a dynamic route

Correct Answer: C
Section:
Explanation:
When remote users connected to FortiSASE require access to internal resources on Branch-2, the following process occurs:
SD-WAN Capability:
FortiSASE leverages SD-WAN to optimize traffic routing based on performance metrics and priorities.
In the priority settings, HUB-1 is configured with the highest priority (P1), whereas HUB-2 has a lower priority (P2).
Traffic Routing Decision:
FortiSASE evaluates the available hubs (HUB-1 and HUB-2) and selects HUB-1 due to its highest priority setting.
Once the traffic reaches HUB-1, it is then routed to the appropriate branch based on internal routing policies.
Branch-2 Access:
Since HUB-1 has the highest priority, FortiSASE directs the traffic to HUB-1.
HUB-1 then routes the traffic to Branch-2, providing the remote users access to the internal resources.
FortiOS 7.2 Administration Guide: Details on SD-WAN configurations and priority settings.
FortiSASE 23.2 Documentation: Explains how FortiSASE integrates with SD-WAN to route traffic based on defined priorities and performance metrics.

QUESTION 3
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

Correct Answer: A, B, D
Section:
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.
FortiOS 7.2 Administration Guide: Details on initial setup and configuration steps for FortiSASE.
FortiSASE 23.2 Documentation: Explains the importance of selecting data center locations for various FortiSASE components.

QUESTION 4
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

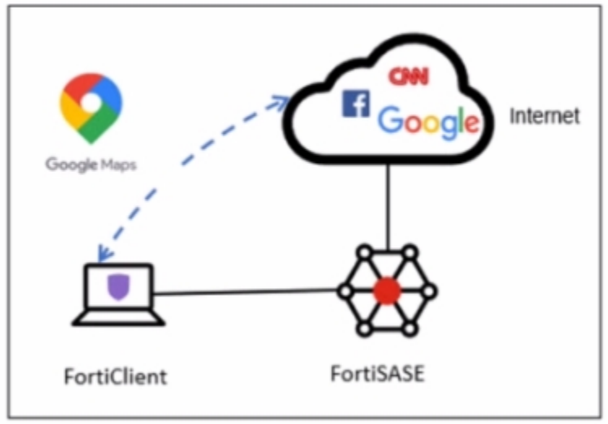
Correct Answer: D
Section:
Explanation:
During FortiSASE provisioning, the FortiSASE administrator needs to configure at least one security point of presence (PoP). A single PoP is sufficient to get started with FortiSASE, providing the necessary security services and connectivity for users.
Security Point of Presence (PoP):
A PoP is a strategically located data center that provides security services such as secure web gateway, firewall, and VPN termination.
Configuring at least one PoP ensures that users can connect to FortiSASE and benefit from its security features.
Scalability:
While only one PoP is required to start, additional PoPs can be added as needed to enhance redundancy, load balancing, and performance.
FortiOS 7.2 Administration Guide: Provides details on the provisioning process for FortiSASE.
FortiSASE 23.2 Documentation: Explains the configuration and role of security PoPs in the FortiSASE architecture.

QUESTION 5
How does FortiSASE hide user information when viewing and analyzing logs?

A. By hashing data using Blowfish
B. By hashing data using salt
C. By encrypting data using Secure Hash Algorithm 256-bit (SHA-256)
D. By encrypting data using advanced encryption standard (AES)

Correct Answer: B
Section:
Explanation:
FortiSASE hides user information when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.
Hashing Data with Salt:
Hashing data involves converting it into a fixed-size string of characters, which is typically a hash value.
Salting adds random data to the input of the hash function, ensuring that even identical inputs produce different hash values.
This method provides enhanced security by making it more difficult to reverse-engineer the original data from the hash value.
Security and Privacy:
Using salted hashes ensures that user information remains secure and private when stored or analyzed in logs.
This technique is widely used in security systems to protect sensitive data from unauthorized access.
FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.
FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

QUESTION 6
Refer to the exhibit.



A company has a requirement to inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE VPN tunnel and redirect it to the endpoint physical Interface.
Which configuration must you apply to achieve this requirement?

A. Exempt the Google Maps FQDN from the endpoint system proxy settings.
B. Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic
C. Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.
D. Change the default DNS server configuration on FortiSASE to use the endpoint system DNS.

Correct Answer: C
Section:
Explanation:
To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass the VPN tunnel and be routed directly through the endpoint's local interface.
Split Tunneling Configuration:
Split tunneling enables selective traffic to be routed outside the VPN tunnel.
By configuring the Google Maps Fully Qualified Domain Name (FQDN) as a split tunneling destination, you ensure that traffic to Google Maps bypasses the VPN tunnel and uses the endpoint's local interface instead.
Implementation Steps:
Access the FortiSASE endpoint profile configuration.
Add the Google Maps FQDN to the split tunneling destinations list.
This configuration directs traffic intended for Google Maps to bypass the VPN tunnel and be routed directly through the endpoint's physical network interface.
FortiOS 7.2 Administration Guide: Provides details on split tunneling configuration.
FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

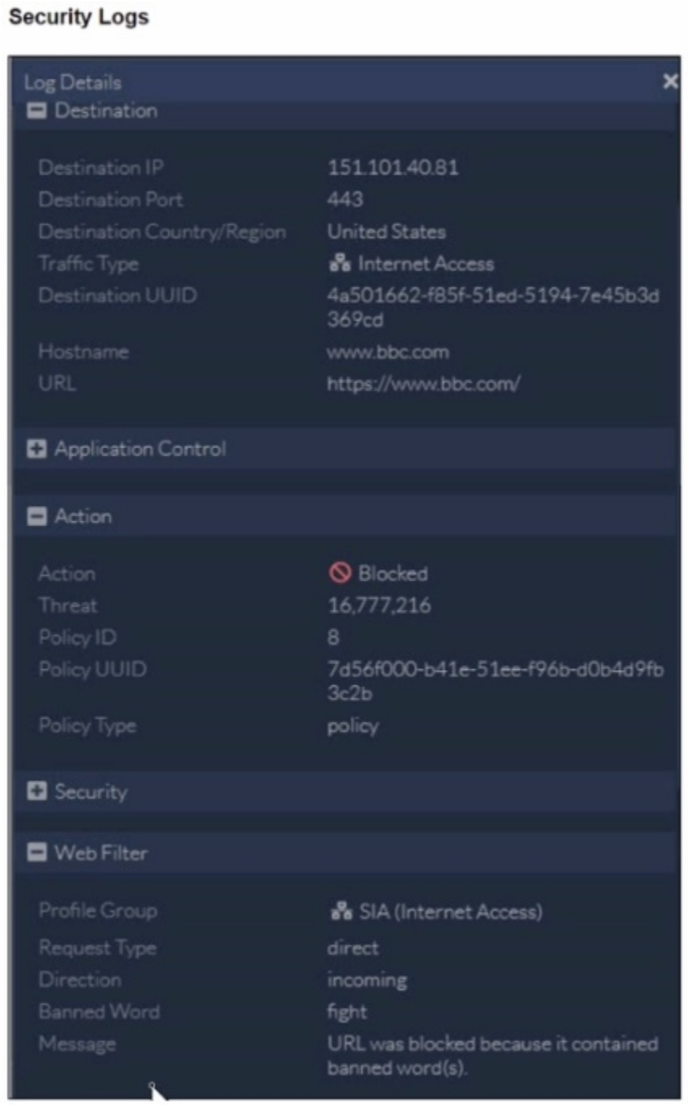
QUESTION 7
Which two advantages does FortiSASE bring to businesses with multiple branch offices? (Choose two.)

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.

Correct Answer: A, D
Section:

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.
FortiOS 7.2 Administration Guide: Provides information on the benefits of centralized management and cloud-based security solutions.
FortiSASE 23.2 Documentation: Explains the advantages of using FortiSASE for businesses with multiple branch offices, including reduced need for on-premises firewalls.

QUESTION 8
Refer to the exhibit.



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

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

Correct Answer: C
Section:
Explanation:
The exhibit indicates that the URL https://www.bbc.com/ is being blocked due to containing a banned word ('fight'). To allow access to this specific URL, you need to adjust the URL filter settings on FortiSASE.
URL Filtering:
URL filtering allows administrators to define policies that block or allow access to specific URLs or URL patterns.
In this case, the URL filter is set to block any URL containing the word 'fight.'
Modifying URL Filter:
Navigate to the Web Filter configuration in FortiSASE.
Locate the URL filter settings.
Add an exception for the URL https://www.bbc.com/ to allow access, even if it contains a banned word.
Alternatively, remove or adjust the banned word list to exclude the word 'fight' if it's not critical to the security policy.
FortiOS 7.2 Administration Guide: Provides details on configuring and managing URL filters.
FortiSASE 23.2 Documentation: Explains how to set up and modify web filtering policies, including URL filters.

QUESTION 9
When you configure FortiSASE Secure Private Access (SPA) with SD-WAN integration, you must establish a routing adjacency between FortiSASE and the FortiGate SD-WAN hub. Which routing protocol must you use?

A. BGP
B. IS-IS
C. OSPF
D. EIGRP

Correct Answer: A
Section:
Explanation:
When configuring FortiSASE Secure Private Access (SPA) with SD-WAN integration, establishing a routing adjacency between FortiSASE and the FortiGate SD-WAN hub requires the use of the Border Gateway Protocol (BGP).
BGP (Border Gateway Protocol):
BGP is widely used for establishing routing adjacencies between different networks, particularly in SD-WAN environments.
It provides scalability and flexibility in managing dynamic routing between FortiSASE and the FortiGate SD-WAN hub.
Routing Adjacency:
BGP enables the exchange of routing information between FortiSASE and the FortiGate SD-WAN hub.
This ensures optimal routing paths and efficient traffic management across the hybrid network.
FortiOS 7.2 Administration Guide: Provides information on configuring BGP for SD-WAN integration.
FortiSASE 23.2 Documentation: Details on setting up routing adjacencies using BGP for Secure Private Access with SD-WAN.

QUESTION 10
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.)

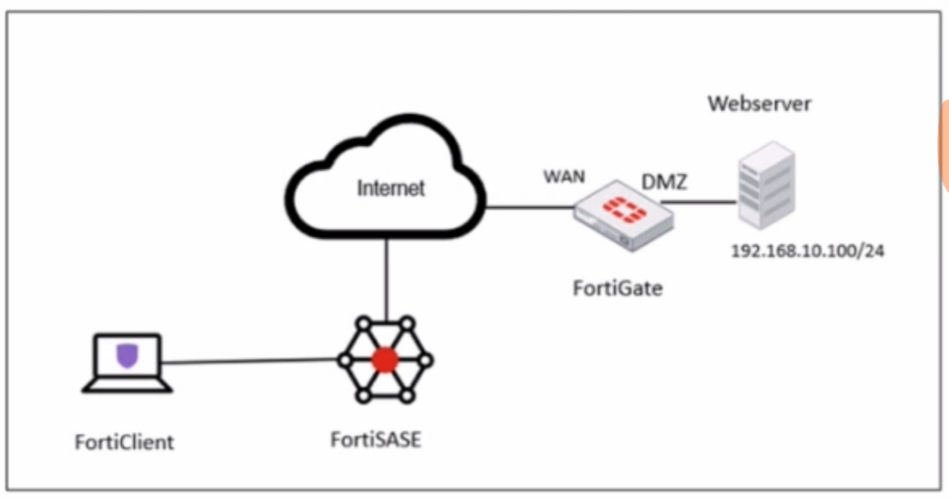
A. Add the FortiGate IP address in the secure private access configuration on FortiSASE.
B. Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE
C. Register FortiGate and FortiSASE under the same FortiCloud account.

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.

Correct Answer: A, B, C
Section:
Explanation:
To configure a Secure Private Access (SPA) solution to share endpoint information between FortiSASE and a corporate FortiGate, you need to take the following steps:
Add the FortiGate IP address in the secure private access configuration on FortiSASE:
This step allows FortiSASE to recognize and establish a connection with the corporate FortiGate.
Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE:
The EMS (Endpoint Management Server) cloud connector facilitates the integration between FortiClient endpoints and FortiSASE, enabling seamless sharing of endpoint information.
Register FortiGate and FortiSASE under the same FortiCloud account:
By registering both FortiGate and FortiSASE under the same FortiCloud account, you ensure centralized management and synchronization of configurations and policies.
FortiOS 7.2 Administration Guide: Provides details on configuring Secure Private Access and integrating with FortiGate.
FortiSASE 23.2 Documentation: Explains how to set up and manage connections between FortiSASE and corporate FortiGate.

QUESTION 11
Refer to the exhibits.

Network diagram

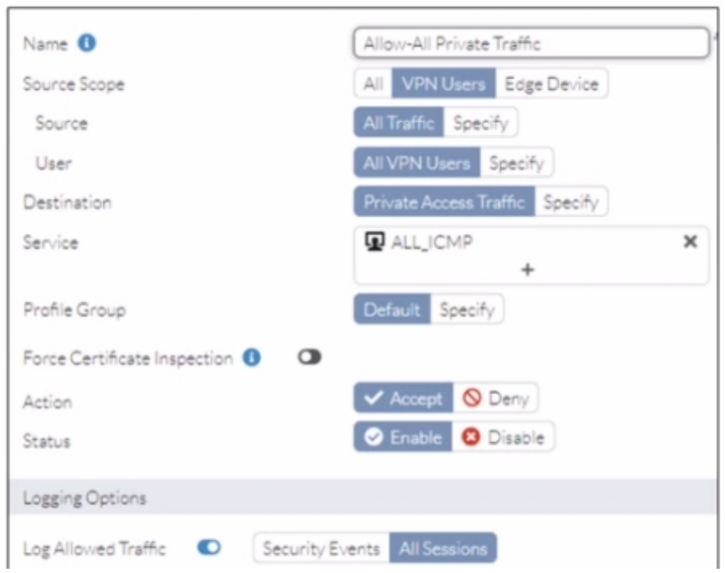


VPN tunnel diagnose output on FortiGate Hub

```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rfc
d=100

parent=SASE index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=s/1
stat: rxp=1667 txp=4583 rxb=278576 txb=108695
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=64916
fec: egress=0 ingress=0
proxyid=SASE proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42025/0B replaywin=1024
       seqno=11cf esn=0 replaywin_lastseq=00000680 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=603df878 esp=aes key=16 2e8932908987c1fdeed9242673bc76f5
       ah=sha1 key=20 01b6c2a13e6cff22796e428c5fb4e4c5262b1a71
  enc: spi=f16ce4a1 esp=aes key=16 90dce5d608caf2714a4f84cff482b557
       ah=sha1 key=20 b60cd0c39489a9f509fe720c0c8e36bb9206f824
  dec:pkts/bytes=3/120, enc:pkts/bytes=2509/285776
  npu_flag=03 npu_rgwy=172.16.10.1 npu_lgwy=172.16.10.101 npu_selid=11 dec_npuid=1 enc_npuid=1
```

Secure Private Access policy on FortiSASE



BGP route information on FortiSASE

Learned BGP Routes

Search

Prefix	Next Hop	Learned From
10.12.11.4/32	0.0.0.0	0.0.0.0
10.12.11.1/32	10.11.11.10	10.11.11.1
10.12.11.2/32	10.11.11.11	10.11.11.1
10.12.11.3/32	10.11.11.12	10.11.11.1
192.168.1.0/24	10.11.11.1	10.11.11.1

Firewall policies on FortiGate Hub

```
# show firewall policy | grep -f SASE
config firewall policy
    edit 5
        set name "vpn_SASE_spoke2hub_0"
        set uuid 01ba85f2-d45c-51ee-5ff9-2035aa36cb3f
        set srcintf "SASE"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "SASE_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 9
        set name "vpn_SASE_spoke2spoke_0"
        set uuid 01eb72ca-d45c-51ee-bd83-bd2feb606cb6
        set srcintf "SASE"
        set dstintf "SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 10
        set name "SASE Health Check"
        set uuid b9573f5c-d45c-51ee-bc11-d5a3143f082a
        set srcintf "SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The tunnel is up to the FortiGale hub. However, the administrator is not able to ping the webserver hosted behind the FortiGate hub. Based on the output, what is the reason for the ping failures?

A. The Secure Private Access (SPA) policy needs to allow PING service.
B. Quick mode selectors are restricting the subnet.

C. The BGP route is not received.
D. Network address translation (NAT) is not enabled on the spoke-to-hub policy.

Correct Answer: B
Section:
Explanation:
The reason for the ping failures is due to the quick mode selectors restricting the subnet. Quick mode selectors define the IP ranges and protocols that are allowed through the VPN tunnel, and if they are not configured correctly, traffic to certain subnets can be blocked.
Quick Mode Selectors:
Quick mode selectors specify the source and destination subnets that are allowed to communicate through the VPN tunnel.
If the selectors do not include the subnet of the webserver (192.168.10.0/24), then the traffic will be restricted, and the ping will fail.
Diagnostic Output:
The diagnostic output shows the VPN configuration details, but it is important to check the quick mode selectors to ensure that the necessary subnets are included.
If the quick mode selectors are too restrictive, they will prevent traffic to and from the specified subnets.
Configuration Check:
Verify the quick mode selectors on both the FortiSASE and FortiGate hub to ensure they match and include the subnet of the webserver.
Adjust the selectors to allow the necessary subnets for successful communication.
FortiOS 7.2 Administration Guide: Provides detailed information on configuring VPN tunnels and quick mode selectors.
FortiSASE 23.2 Documentation: Explains how to set up and manage VPN tunnels, including the configuration of quick mode selectors.

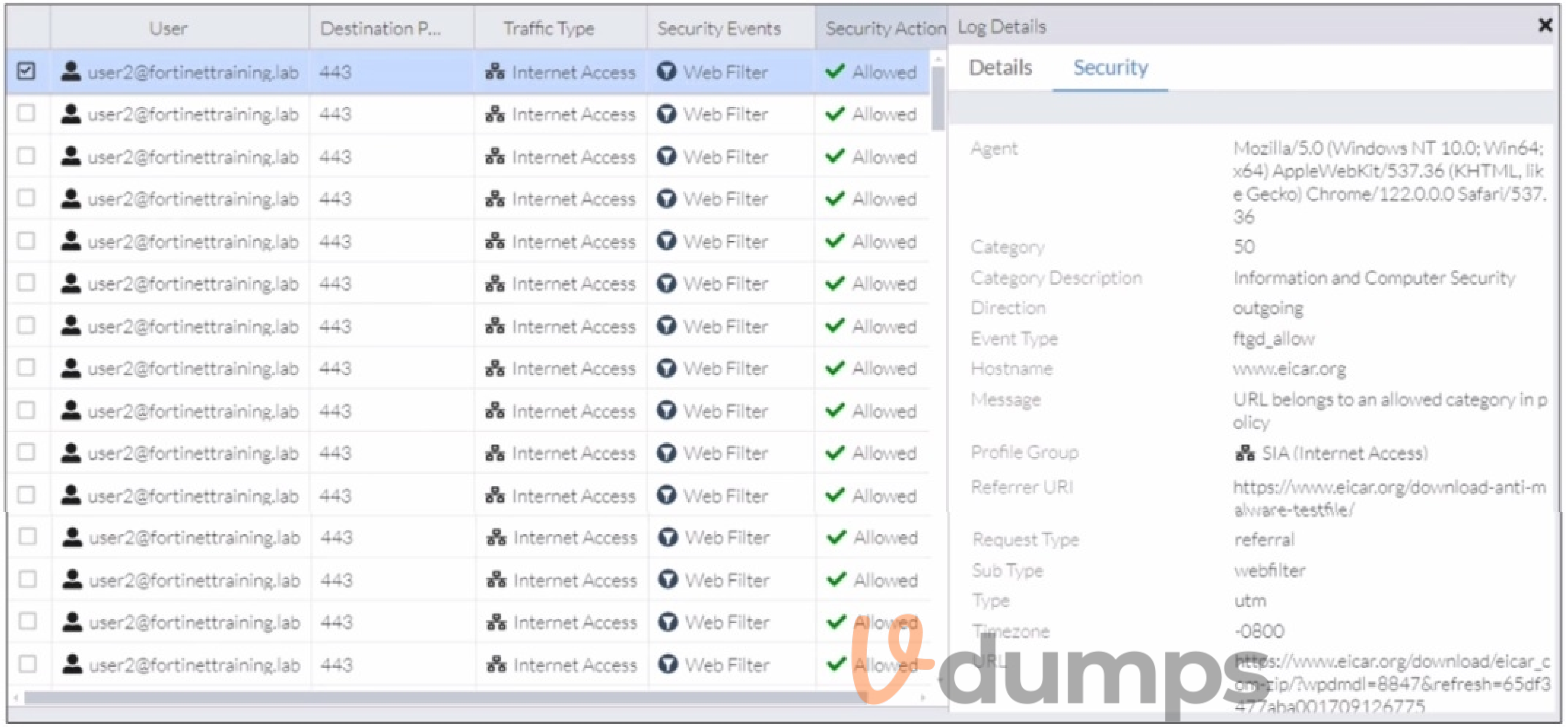
QUESTION 12
To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

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

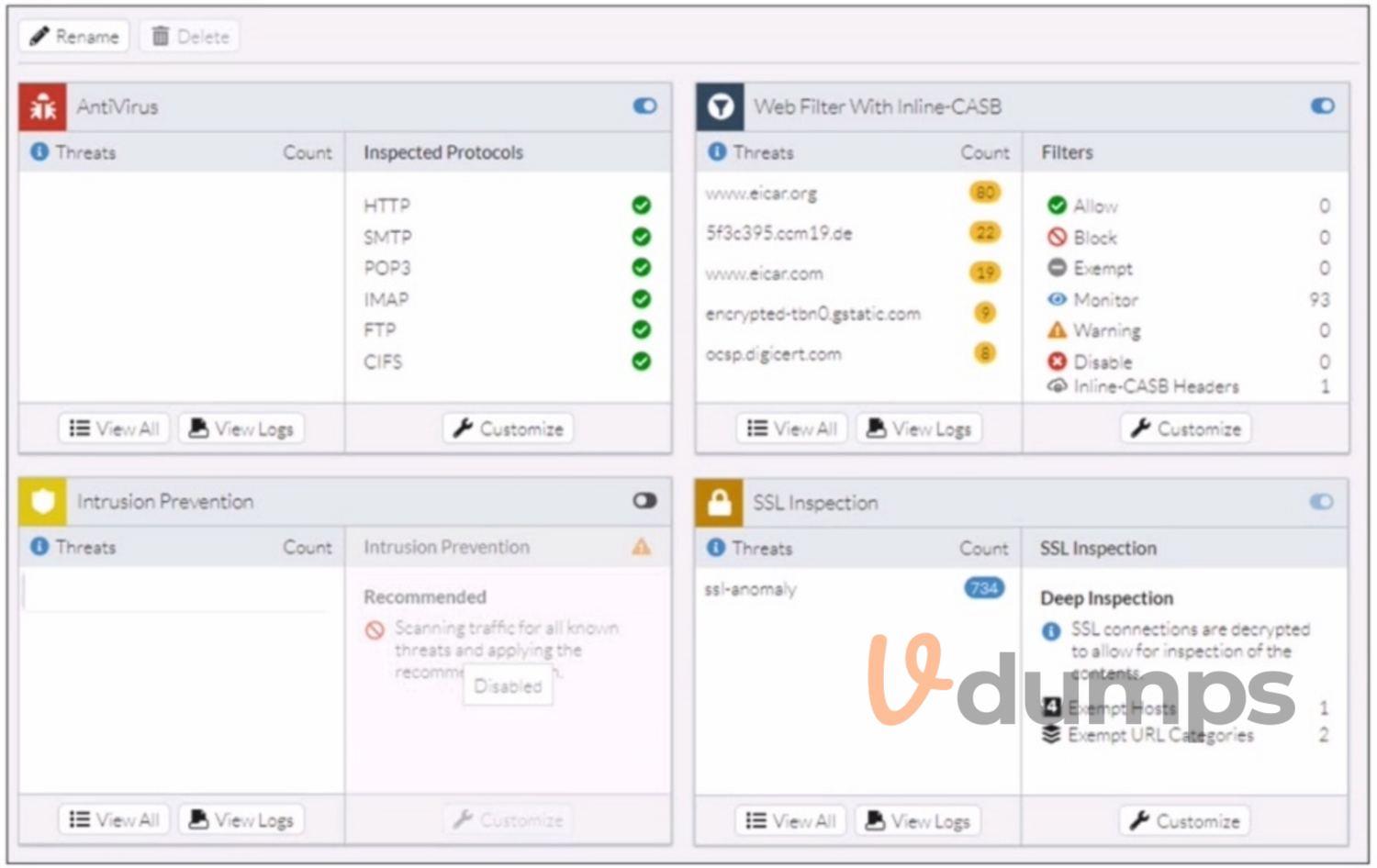
Correct Answer: C
Section:
Explanation:
Zero Trust Network Access (ZTNA) private access provides the most efficient and secure method for remote users to access a TCP-based application hosted on a private web server. ZTNA ensures that only authenticated and authorized users can access specific applications based on predefined policies, enhancing security and access control.
Zero Trust Network Access (ZTNA):
ZTNA operates on the principle of 'never trust, always verify,' continuously verifying user identity and device security posture before granting access.
It provides secure and granular access to specific applications, ensuring that remote users can securely access the TCP-based application hosted on the private web server.
Secure and Efficient Access:
ZTNA private access allows remote users to connect directly to the application without needing a full VPN tunnel, reducing latency and improving performance.
It ensures that only authorized users can access the application, providing robust security controls.
FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its deployment use cases.
FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

QUESTION 13
Refer to the exhibits.

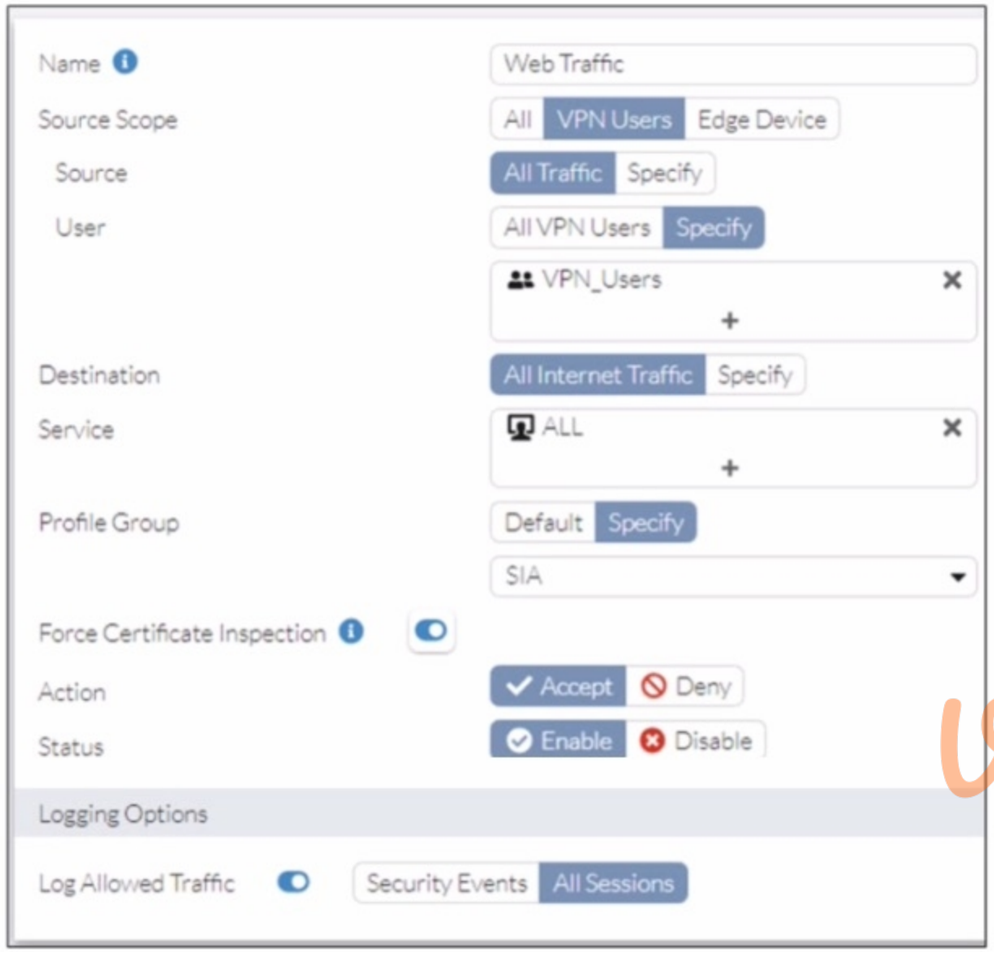
Web Filtering logs



Security Profile Group



Secure Internet Access policy



A FortiSASE administrator has configured an antivirus profile in the security profile group and applied it to the internet access policy. Remote users are still able to download the eicar.com-zip file from https://eicar.org. Traffic logs show traffic is allowed by the policy.
Which configuration on FortiSASE is allowing users to perform the download?

A. Web filter is allowing the traffic.
B. IPS is disabled in the security profile group.
C. The HTTPS protocol is not enabled in the antivirus profile.
D. Force certificate inspection is enabled in the policy.

Correct Answer: A
Section:
Explanation:
Based on the provided exhibits and the configuration details, the reason why users are still able to download the eicar.com-zip file despite having an antivirus profile applied is due to the Web Filter allowing the traffic. Here is the step-by-step detailed explanation:
Web Filtering Logs Analysis:
The logs show that the traffic to the destination port 443 (which is HTTPS) is allowed and the security event triggered is Web Filter.
The log details indicate that the URL belongs to an allowed category in the policy and thus, the traffic is permitted by the Web Filter.
Security Profile Group Configuration:

The Web Filter with Inline-CASB section indicates that the site www.eicar.org is being monitored (93 occurrences) and not blocked.
Since the Web Filter is set to allow traffic from this site, the antivirus profile will not block it because the Web Filter decision takes precedence.
Antivirus Profile Configuration:
Although the antivirus profile is configured, the logs do not show any antivirus actions being triggered. This indicates that the web filter is overriding the antivirus action.
Policy Configuration:
The policy named 'Web Traffic' shows that it has logging enabled and is set to accept traffic.
The profile group 'SIA' applied to this policy includes both Web Filter and Antivirus settings. However, since the Web Filter is allowing the traffic, the antivirus profile does not get the chance to inspect it.
FortiGate Security 7.2 Study Guide: Provides details on the precedence of web filtering over antivirus in security profiles.
Fortinet Knowledge Base: Detailed explanation of web filtering and antivirus profiles interaction.

QUESTION 14
An organization wants to block all video and audio application traffic but grant access to videos from CNN Which application override action must you configure in the Application Control with Inline-CASB?

A. Allow
B. Pass
C. Permit
D. Exempt

Correct Answer: D
Section:
Explanation:
To block all video and audio application traffic while granting access to videos from CNN, you need to configure an application override action in the Application Control with Inline-CASB. Here is the step-by-step detailed explanation:
Application Control Configuration:
Application Control is used to identify and manage application traffic based on predefined or custom application signatures.
Inline-CASB (Cloud Access Security Broker) extends these capabilities by allowing more granular control over cloud applications.
Blocking Video and Audio Applications:
To block all video and audio application traffic, you can create a policy within Application Control to deny all categories related to video and audio streaming.
Granting Access to Specific Videos (CNN):
To allow access to videos from CNN specifically, you must create an override rule within the same Application Control profile.
The override action 'Exempt' ensures that traffic to specified URLs (such as those from CNN) is not subjected to the blocking rules set for other video and audio traffic.
Configuration Steps:
Navigate to the Application Control profile in the FortiSASE interface.
Set the application categories related to video and audio streaming to 'Block.'
Add a new override entry for CNN video traffic and set the action to 'Exempt.'
FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.
Fortinet Training Institute: Provides scenarios and examples of using Application Control with Inline-CASB for specific use cases.

QUESTION 15
Which policy type is used to control traffic between the FortiClient endpoint to FortiSASE for secure internet access?

A. VPN policy
B. thin edge policy
C. private access policy
D. secure web gateway (SWG) policy

Correct Answer: D
Section:
Explanation:

The Secure Web Gateway (SWG) policy is used to control traffic between the FortiClient endpoint and FortiSASE for secure internet access. SWG provides comprehensive web security by enforcing policies that manage and monitor user access to the internet.
Secure Web Gateway (SWG) Policy:
SWG policies are designed to protect users from web-based threats and enforce acceptable use policies.
These policies control and monitor user traffic to and from the internet, ensuring that security protocols are followed.
Traffic Control:
The SWG policy intercepts all web traffic, inspects it, and applies security rules before allowing or blocking access.
This policy type is crucial for providing secure internet access to users connecting through FortiSASE.
FortiOS 7.2 Administration Guide: Details on configuring and managing SWG policies.
FortiSASE 23.2 Documentation: Explains the role of SWG in securing internet access for endpoints.

QUESTION 16
Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	use2@fortinettraining.lab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	use1@fortinettraining.lab	Online	FortiSASE-Non-Compliant,FortiSASE-Compliant	7.0.8.0427	176

Secure Internet Access Policy

Create | Edit | Delete | Search

Name	Profile Group	Source	User	Destination	Action
Botnet Deny		all	All VPN Users	Botnet-C&C.Server	Deny
Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
Allow-All	Default		All VPN Users	All Internet Traffic	Accept
Implicit Deny		all	All VPN Users	All Internet Traffic	Deny

WiMO-Pro and Win7-Pro are endpoints from the same remote location. WiMO-Pro can access the internet though FortiSASE, while Wm7-Pro can no longer access the internet
Given the exhibits, which reason explains the outage on Wm7-Pro?

A. The Win7-Pro device posture has changed.
B. Win7-Pro cannot reach the FortiSASE SSL VPN gateway
C. The Win7-Pro FortiClient version does not match the FortiSASE endpoint requirement.
D. Win-7 Pro has exceeded the total vulnerability detected threshold.

Correct Answer: D
Section:
Explanation:
Based on the provided exhibits, the reason why the Win7-Pro endpoint can no longer access the internet through FortiSASE is due to exceeding the total vulnerability detected threshold. This threshold is used to determine if a device is compliant with the security requirements to access the network.
Endpoint Compliance:

FortiSASE monitors endpoint compliance by assessing various security parameters, including the number of vulnerabilities detected on the device.
The compliance status is indicated by the ZTNA tags and the vulnerabilities detected.
Vulnerability Threshold:
The exhibit shows that Win7-Pro has 176 vulnerabilities detected, whereas Win10-Pro has 140 vulnerabilities.
If the endpoint exceeds a predefined vulnerability threshold, it may be restricted from accessing the network to ensure overall network security.
Impact on Network Access:
Since Win7-Pro has exceeded the vulnerability threshold, it is marked as non-compliant and subsequently loses internet access through FortiSASE.
The FortiSASE endpoint profile enforces this compliance check to prevent potentially vulnerable devices from accessing the internet.
FortiOS 7.2 Administration Guide: Provides information on endpoint compliance and vulnerability management.
FortiSASE 23.2 Documentation: Explains how vulnerability thresholds are used to determine endpoint compliance and access control.

QUESTION 17
A customer wants to upgrade their legacy on-premises proxy to a could-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

A. SD-WAN and NGFW
B. SD-WAN and inline-CASB
C. zero trust network access (ZTNA) and next generation firewall (NGFW)
D. secure web gateway (SWG) and inline-CASB

Correct Answer: D
Section:
Explanation:
For a customer looking to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network, the combination of Secure Web Gateway (SWG) and Inline Cloud Access Security Broker (CASB) features in FortiSASE will provide the necessary capabilities.
Secure Web Gateway (SWG):
SWG provides comprehensive web security by inspecting and filtering web traffic to protect against web-based threats.
It ensures that all web traffic, whether originating from on-premises or remote locations, is inspected and secured by the cloud-based proxy.
Inline Cloud Access Security Broker (CASB):
CASB enhances security by providing visibility and control over cloud applications and services.
Inline CASB integrates with SWG to enforce security policies for cloud application usage, preventing unauthorized access and data leakage.
FortiOS 7.2 Administration Guide: Details on SWG and CASB features.
FortiSASE 23.2 Documentation: Explains how SWG and inline-CASB are used in cloud-based proxy solutions.

QUESTION 18
Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles9

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.

Correct Answer: C
Section:
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.
FortiOS 7.2 Administration Guide: Provides information on ZTNA and endpoint security posture checks.
FortiSASE 23.2 Documentation: Details on how FortiSASE implements ZTNA principles.