Fortinet.NSE7_SSE_AD-25.v2026-11-09.q39

Exam Code:	NSE7_SSE_AD-25
Exam Name:	Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator
Certification Provider:	Fortinet
Free Question Number:	39
Version:	v2026-11-09
# of views:	106
# of Questions views:	392
https://www.freecram.net/torrent/Fortinet.NSE7_SSE_AD-25.v2026-11-09.q39.html	

NEW QUESTION: 1
When viewing the daily summary report generated by FortiSASE. the administrator notices that the report contains very little data. What is a possible explanation for this almost empty report?
A. Digital experience monitoring is not configured.
B. Log allowed traffic is set to Security Events for all policies.
C. The web filter security profile is not set to Monitor
D. There are no security profile group applied to all policies.
Answer: (SHOW ANSWER)
If the daily summary report generated by FortiSASE contains very little data, one possible explanation is that the "Log allowed traffic" setting is configured to log only "Security Events" for all policies. This configuration limits the amount of data logged, as it only includes security events and excludes normal allowed traffic.
* Log Allowed Traffic Setting:
* The "Log allowed traffic" setting determines which types of traffic are logged.
* When set to "Security Events," only traffic that triggers a security event (such as a threat detection or policy violation) is logged.
* Impact on Report Data:
* If the log setting excludes regular allowed traffic, the amount of data captured and reported is significantly reduced.
* This results in reports with minimal data, as only security-related events are included.
References:
FortiOS 7.6 Administration Guide: Provides details on configuring logging settings for traffic policies.
FortiSASE 23.2 Documentation: Explains the impact of logging configurations on report generation and data visibility.

NEW QUESTION: 2
What are two benefits of deploying FortiSASE with FortiGate ZTNA access proxy? (Choose two answers)
A. The on-premises FortiGate performs a device posture check.
B. It is ideal for latency-sensitive applications.
C. It supports both agentless ZTNA and agent-based ZTNA.
D. It offers data center redundancy.

Answer: (SHOW ANSWER)
The correct answers are A and B . In the FortiGate ZTNA access proxy workflow, FortiSASE and FortiClient first exchange endpoint information, user login details, security posture, and certificate information.
FortiSASE then synchronizes the FortiClient certificate and security posture tags with FortiGate. The study guide states that FortiGate verifies the certificate, performs a user check, and performs a posture check based on the security posture tags before allowing encrypted access to the protected applications. This directly supports option A.
Option B is also correct because the ZTNA access proxy provides a direct path to private resources.
The guide describes the ZTNA access proxy use case as a direct connection to applications hosted behind FortiGate, with a TLS-encrypted tunnel automatically created from the endpoint to the access proxy. It further states that this use case offers the direct shortest path to private resources, improving performance and security. That makes it suitable for latency-sensitive applications. Option C is incorrect because this specific FortiGate ZTNA access proxy deployment requires FortiClient on endpoints; agentless ZTNA is handled separately through the FortiSASE agentless ZTNA portal.
Option D is not stated as a benefit of this deployment model.

NEW QUESTION: 3
An existing Fortinet SD-WAN customer is reviewing the FortiSASE ordering guide to identify which add-on is needed to allow future FortiSASE remote users to reach private resources. Which add-on should the customer consider to allow private access? (Choose one answer)
A. FortiSASE Global add-on
B. FortiSASE Branch On-Ramp add-on
C. FortiSASE SPA add-on
D. FortiSASE Dedicated Public IP Address add-on
Answer: (SHOW ANSWER)
To enable remote users to access internal applications located behind an existing FortiGate SD-WAN hub, the customer must license the FortiSASE Secure Private Access (SPA) add-on .
* Secure Private Access (SPA) Use Case: This specific add-on is designed to extend the Fortinet Security Fabric into the SASE cloud, allowing for a hub-and-spoke architecture where the FortiSASE PoPs act as spokes and the customer ' s on-premises FortiGate acts as the hub.
* Licensing Requirements: The SPA add-on is a per-hub (per service connection) license. It provides the necessary entitlements to establish IPsec tunnels and BGP peering between the SASE infrastructure and the corporate FortiGate.
* Feature Enablement: Once the SPA license is applied, the Configuration > Private Access menu becomes available in the FortiSASE portal. This allows administrators to define " Service Connections
" to their private data centers or cloud VPCs.
* Analysis of Other Options:
* Option A: The Global add-on is typically related to expanding the geographic reach or performance of the SASE PoPs, not specifically for private resource routing.
* Option B: The Branch On-Ramp refers to connecting physical office locations (Thin Edge) to SASE, rather than the specific licensing for private application access for remote users.
* Option D: Dedicated Public IP Address is used for source IP anchoring (SIA) to ensure remote users egress with a consistent IP for third-party SaaS IP-whitelisting.

NEW QUESTION: 4
A FortiSASE administrator is receiving reports that some users have travelled overseas and cannot establish their agent-based VPN tunnels, although they can authenticate with their SSO credentials to access O365 and SFDC directly. The administrator reviewed the firewall policies and ZTNA tags of some users and could not find anything unusual. Which action can the administrator take to resolve this problem? (Choose one answer)
A. Create a dedicated firewall policy for the users.
B. Instruct the users to restart their laptops and log in again.
C. Ensure that the countries the users are visiting are not listed under the Deny list in the Geofencing settings.
D. Instruct the users to install the updated version of the agent-based client.
Answer: (SHOW ANSWER)
In a FortiSASE environment, the ability of a remote user to establish a VPN tunnel is governed not only by their credentials and firewall policies but also by geographic access controls .
* Geofencing Mechanism: FortiSASE includes a Geofencing feature (found under Configuration > Restrictions or Configuration > Geofencing in newer versions) that allows administrators to restrict or allow access to SASE services based on the geographic location of the endpoint ' s public IP address.
* Connection Failure vs. SSO Success: The scenario describes a situation where users can successfully authenticate via SSO to reach third-party SaaS apps like Office 365 (O365) or Salesforce (SFDC) but cannot connect to the SASE VPN. This occurs because the SSO authentication is handled directly by the Identity Provider (IdP) (e.g., Microsoft Entra ID), which may not have the same geographic restrictions. However, when the FortiClient attempts to establish the tunnel to the FortiSASE Point of Presence (PoP), the SASE gateway checks the Geofencing list . If the country the user is visiting is on the Deny list (or not on the Allow list), the connection is dropped at the " local-in " policy level on the SASE backend, preventing the tunnel from forming.
* Verification and Resolution: To resolve this, the administrator must verify the Geofencing settings and ensure that the countries where the traveling users are located are permitted to connect. If the feature is enabled with a " Deny " list, the specific country must be removed from that list; if it uses an " Allow " list, the country must be added.
* Analysis of Other Options:
* Option A: Firewall policies govern traffic after the tunnel is established; they cannot resolve a failure to connect the tunnel itself.
* Option B: Restarting the device is a general troubleshooting step but will not bypass a server- side geographic block.
* Option D: While keeping clients updated is a best practice, the issue described (specific to overseas travel while other functions work) points to a configuration restriction rather than a software bug.

NEW QUESTION: 5
Your organization is currently using FortiSASE for its cybersecurity. They have recently hired a contractor who will work from the HQ office and who needs temporary internet access in order to set up a web-based point of sale (POS) system. How can you provide secure internet access to the contractor using FortiSASE?
(Choose one answer)
A. Use a proxy auto-configuration (PAC) file and provide secure web gateway (SWG) service as an explicit web proxy.
B. Use a tunnel policy with a contractors user group as the source on FortiSASE to provide internet access.
C. Use zero trust network access (ZTNA) and tag the client as an unmanaged endpoint.
D. Use the self-registration portal on FortiSASE to grant internet access.
Answer: (SHOW ANSWER)
In the FortiSASE architecture, there are two primary methods for delivering Secure Internet Access (SIA):

Agent-based (using FortiClient) and Agentless (using Secure Web Gateway/SWG).
* Use Case Analysis: The scenario describes a contractor-an unmanaged user-who requires temporary access for a web-based application (the POS system). For contractors or guests using personal/non-corporate devices where installing the FortiClient agent is either not feasible or not desired, FortiSASE provides the SIA Agentless deployment model.
* Mechanism (SWG & PAC): In this mode, FortiSASE functions as an explicit web proxy. To steer the contractor's web traffic (HTTP/HTTPS) to the SASE cloud for inspection, the administrator provides the user with a proxy auto-configuration (PAC) file. The contractor simply configures their browser or operating system to point to the URL of this PAC file.
* Security Enforcement: Once the PAC file is applied, all web traffic from the contractor's device is redirected to the FortiSASE SWG PoP. Here, the traffic is subject to the organization's full security stack, including SSL deep inspection, Antivirus, Web Filtering, and Application Control, ensuring that even temporary contractor access is fully secured and logged.
* Why other options are incorrect:
* Option B (Tunnel Policy): This refers to agent-based access where a VPN tunnel is established.
This requires FortiClient, which is generally not used for temporary contractors on unmanaged devices.
* Option C (ZTNA Unmanaged): While ZTNA supports agentless access to private applications (SPA), providing internet access (SIA) to an unmanaged endpoint is specifically the role of the SWG/Proxy service.
* Option D (Self-registration): While FortiSASE has a User Portal for onboarding, it is a method for user registration/credential management, not the technical traffic-steering mechanism used to provide internet connectivity.
According to the FortiSASE 25 Secure Internet Access Architecture Guide, the SWG (Agentless) approach is the recommended best practice for securing web-only traffic from unmanaged endpoints and third- party contractors.

NEW QUESTION: 6
Which two benefits come from integrating SoCaaS with FortiSASE? (Choose two answers)
A. Eliminates the need of endpoint projection software
B. Continuous threat monitoring of all connected endpoints
C. Centralized visibility of all threat events
D. Provides bandwidth usage analytics
Answer: (SHOW ANSWER)
The integration of FortiGuard SOCaaS with FortiSASE significantly strengthens an organization's security posture by offloading complex security operations to Fortinet's expert analysts.4
* Continuous Threat Monitoring (B): FortiGuard SOCaaS provides 24x7x365 threat monitoring for all endpoints connected to the FortiSASE environment. This service eliminates the need for organizations to hire and maintain their own round-the-clock security operations staff while ensuring that threats are detected and verified in as little as 15 minutes.
* Centralized Visibility (C): By forwarding FortiSASE logs to the SOCaaS cloud, administrators gain centralized visibility of all security events through a single, user-friendly portal. This portal allows security teams to track threats, review expert-led incident escalations, and communicate directly with Fortinet SOC analysts to streamline the incident response process.
* Operational Efficiency: The integration uses AI-driven alert triage and automated correlation to distill data from the Fortinet Security Fabric, focusing on legitimate threats and reducing the alert fatigue often experienced by internal IT teams.

NEW QUESTION: 7
How does FortiSASE Secure Private Access (SPA) facilitate connectivity to private resources in a hub-and- spoke network? (Choose one answer)

A. SPA applies source network address translation (SNAT) for remote user traffic and uses IKEv1 for IPsec tunnels to connect to standalone hubs without BGP support.
B. SPA connects to private resources using HTTP and HTTPS protocols and relies on FortiClient for agentless access to SD-WAN deployments.
C. SPA establishes direct links to spokes without IPsec or BGP and uses an easy configuration key to secure web traffic for remote users.
D. SPA connects a FortiSASE POP to a FortiGate hub or SD-WAN deployment using IPsec and BGP for dynamic route exchange, with an easy configuration key for simplified setup on FortiOS.
Answer: (SHOW ANSWER)
The correct answer is D . The FortiSASE study guide explains that SPA allows a FortiSASE POP to act as a spoke and connect to a FortiGate hub. It states that you can use FortiSASE SPA so that a POP connects to either a standalone hub using IPsec or to an existing Fortinet SD-WAN deployment . It also states that the BGP protocol is established through IPsec links for dynamic route exchange, which gives FortiSASE remote users access to private resources. For hub deployments running FortiOS 7.4.5 or later, the guide explains that an easy configuration key can simplify SPA setup on FortiSASE by automatically populating key fields in the FortiGate hub configuration.
The wrong options contradict the guide. Option A is false because FortiSASE does not apply SNAT for remote VPN user and edge device traffic destined for SPA hubs, and FortiSASE spokes support IKEv2, not IKEv1. Option B confuses agentless ZTNA with SD-WAN private access. Option C is wrong because SPA uses IPsec and BGP, and the easy configuration key is for SPA hub setup, not for securing general web traffic.

NEW 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
Answer: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 9

Which two statements about the Hub Selection Method in FortiSASE Secure Private Access (SPA) are correct? (Choose two answers)

A. When using Hub Health and Priority, FortiSASE selects the highest priority hub that meets the configured SLA thresholds.

B. When using BGP MED, FortiSASE selects the hub with the lowest MED value only if it also meets the configured SLA thresholds.

C. When using SLA thresholds, administrators can customize latency, jitter, and packet loss for each security POP.

D. When using Hub Health and Priority, all hubs with the same priority are always selected regardless of SLA results.

Answer: (SHOW ANSWER)

According to the NSE7 SASE Enterprise Guide (Pages 64 & 153) , FortiSASE utilizes an intelligent engine to manage connectivity to private resources through various selection methods:

* Hub Health and Priority: FortiSASE incorporates a built-in SD-WAN engine for intelligent routing selection among established IPsec links. The health check IP address periodically receives performance metrics, including jitter, latency, and packet loss, for each service connection. In this mode, FortiSASE evaluates the available hubs and selects the one with the highest priority (the most preferred value) within each POP, provided that the hub meets the defined service-level agreement (SLA) requirements . For this configuration to function correctly, both FortiSASE and the SPA hub must use the same Autonomous System Number (ASN).

* BGP Multiple Exit Discriminator (MED): This method leverages the standard BGP MED attribute, which allows an autonomous system to signal its preferred entry point to a peer. FortiSASE learns the MED values advertised by the configured hubs. The architecture is designed so that the lower the MED value , the more preferred the path is to the receiving router. Consistent with the " Zero Trust " and " Secure Access " principles, even when using BGP MED, the selection is gated by the health engine; therefore, the hub is only selected if it also satisfies the configured SLA thresholds .

While SLA thresholds can be configured, the primary logic for hub selection focuses on how priority and dynamic routing attributes (like MED) interact with the real-time health of the tunnel.

NEW QUESTION: 10

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?

Freecram.net

A. BGP

B. IS-IS

C. OSPF

D. EIGRP

Answer: (SHOW ANSWER)

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.

References:

FortiOS 7.6 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.

NEW QUESTION: 11
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. 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: (SHOW ANSWER)

The VPN tunnel between the FortiSASE spoke and the FortiGate hub is not establishing due to the configuration of mode config, which is not supported by FortiSASE spoke devices. Mode config is used to assign IP addresses to VPN clients dynamically, but this feature is not applicable to FortiSASE spokes.

* Mode Config in IPsec:
* The configuration snippet shows that mode config is enabled in the IPsec phase 1 settings.
* Mode config is typically used for VPN clients to dynamically receive an IP address from the VPN server, but it is not suitable for site-to-site VPN configurations involving FortiSASE spokes.
* Configuration Adjustment:
* To establish the VPN tunnel, you need to disable mode config in the IPsec phase 1 settings.
* This adjustment will allow the FortiSASE spoke to properly establish the VPN tunnel with the FortiGate hub.
* Steps to Disable Mode Config:
* Access the VPN configuration on the FortiSASE spoke.
* Edit the IPsec phase 1 settings to disable mode config.
* Ensure other settings such as pre-shared key, remote gateway, and BGP configurations are correct and consistent with the FortiGate hub.

References:

FortiOS 7.6 Administration Guide: Provides details on configuring IPsec VPNs and mode config settings.

FortiSASE 23.2 Documentation: Explains the supported configurations for FortiSASE spoke devices and VPN setups.

NEW QUESTION: 12

You are designing a new network, and the cybersecurity policy mandates that all remote users working from home must always be connected and protected. Which FortiSASE component facilitates this always-on security measure? (Choose one answer)

A. Unified FortiClient

B. SDWAN on-ramp2

C. Secure web gateway

D. Thin-branch SASE extension

Answer: (SHOW ANSWER)

In a FortiSASE environment, the Unified FortiClient agent is the critical component that fulfills the requirement for " always-on " connectivity and security for remote users.

* Persistent Encrypted Tunnels : The Unified FortiClient maintains a persistent, always-on connection to the FortiSASE infrastructure. 4 This is typically achieved through an auto-connect VPN tunnel (SSL or IPsec) that initiates as soon as the user logs into their device and has internet access.
* Continuous Security Enforcement : By staying connected to a nearby FortiSASE Point of Presence (PoP), the endpoint ensures that all traffic is inspected. This allows the organization to enforce a consistent security posture-including Web Filtering, Antivirus, and Application Control-regardless of whether the user is at home, in a coffee shop, or traveling.

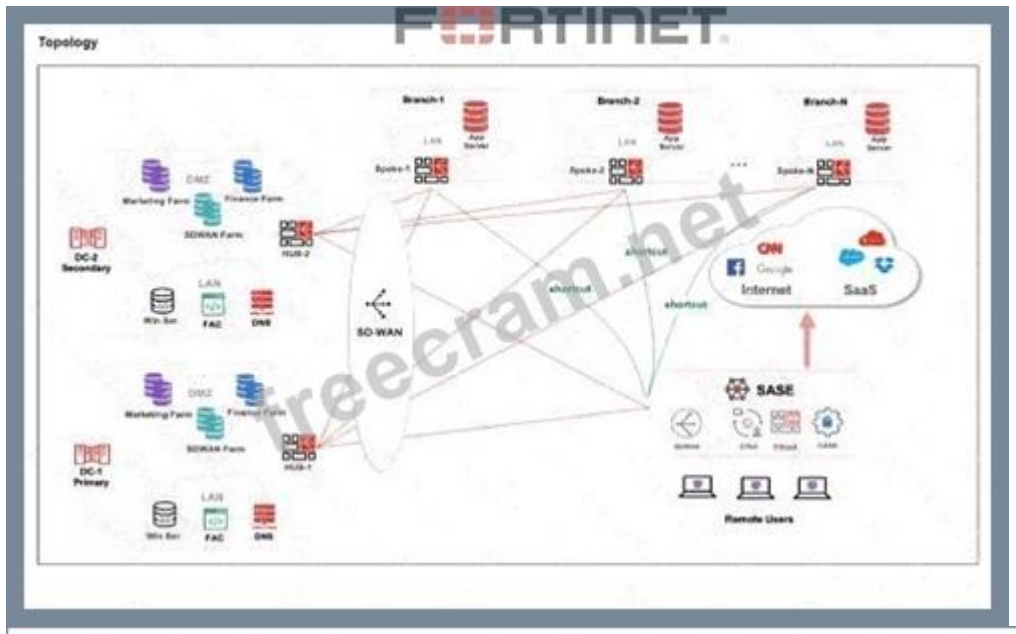
* Zero-Trust Integration : Beyond simple connectivity, the unified agent supports Universal ZTNA . It continuously verifies the identity of the user and the security posture of the device before granting access to specific applications, thereby satisfying modern zero-trust security mandates.
* Comparison of Other Components :
* SD-WAN on-ramp (B) : Used primarily to integrate existing branch office SD-WAN networks with the SASE cloud for private application access.
* Secure Web Gateway (C) : While a feature of the SASE PoP, the agentless SWG deployment (using PAC files) does not provide the same level of " always-on " persistent tunnel protection as the FortiClient agent.
* Thin-branch SASE extension (D) : Focused on securing small branch locations (using FortiAP or FortiExtender) where individual client agents may not be deployed on every device.

NEW QUESTION: 13
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
Answer: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 14
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: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 15
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

Answer: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 16
You are designing a new network for Company X and one of the new cybersecurity policy requirements is that all remote user endpoints must always be connected and protected Which FortiSASE component facilitates this always-on security measure?
A. site-based deployment
B. thin-branch SASE extension
C. unified FortiClient
D. inline-CASB
Answer: (SHOW ANSWER)
The unified FortiClient component of FortiSASE facilitates the always-on security measure required for ensuring that all remote user endpoints are always connected and protected.
* Unified FortiClient:
* FortiClient is a comprehensive endpoint security solution that integrates with FortiSASE to provide continuous protection for remote user endpoints.
* It ensures that endpoints are always connected to the FortiSASE infrastructure, even when users are off the corporate network.
* Always-On Security:
* The unified FortiClient maintains a persistent connection to FortiSASE, enforcing security policies and protecting endpoints against threats at all times.
* This ensures compliance with the cybersecurity policy requiring constant connectivity and protection for remote users.
References:
FortiOS 7.6 Administration Guide: Provides information on configuring and managing FortiClient for endpoint security.
FortiSASE 23.2 Documentation: Explains how FortiClient integrates with FortiSASE to deliver always-on security for remote endpoints.

Valid NSE7_SSE_AD-25 Dumps shared by ExamDiscuss.com for Helping Passing NSE7_SSE_AD-25 Exam! ExamDiscuss.com now offer the **newest NSE7_SSE_AD-25 exam dumps**, the ExamDiscuss.com NSE7_SSE_AD-25 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com NSE7_SSE_AD-25 dumps with Test Engine here: https://www.examdiscuss.com/Fortinet/exam/NSE7_SSE_AD-25/premium/ (**109** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
Which two settings are automatically pushed from FortiSASE to FortiClient in a new FortiSASE deployment with default settings? (Choose two answers)
A. FortiSASE certificate authority (CA) certificate
B. Tunnel profile
C. Real-time protection
D. Zero trust network access (ZTNA) tags1
Answer: (SHOW ANSWER)
In a standard FortiSASE agent-based deployment, the FortiSASE Endpoint Management Service (EMS) acts as the central control plane for all managed FortiClient instances. When an endpoint is onboarded, the system is designed to provide " zero-touch " configuration for the core connectivity and security components.
* CA Certificate (A): For SSL deep inspection to function without triggering browser certificate warnings, the endpoint must trust the FortiSASE CA. FortiSASE supports automatically installing the FortiSASE CA certificate for managed agent-based users. Once the endpoint connects to the FortiSASE EMS, the service automatically deploys the CA certificate to the trusted certificate store of the client machine.
* Tunnel Profile (B): To enable Secure Internet Access (SIA), FortiClient requires a pre-configured VPN or tunnel profile that points to the FortiSASE cloud infrastructure. In a new deployment with default settings, FortiSASE automatically pushes the tunnel profile (including gateway information and auto-connect settings) to the FortiClient endpoint. This allows the user to establish a full-tunnel connection to the nearest Security PoP immediately after onboarding.
* Analysis of Incorrect Options:
* Real-time protection (C): While FortiSASE can manage Malware Protection and Sandbox settings, specific " Real-time protection " features often require manual activation or specific configuration within the Malware Protection profile before being pushed; they are not necessarily
" automatically " active in the absolute default state without a profile assignment.
* ZTNA tags (D): ZTNA tags are dynamic security posture attributes. While FortiSASE evaluates the endpoint to determine which tags apply, the tags themselves are not " pushed " to the client as a setting; rather, the ZTNA connection rules are pushed, and the tags are synchronized back to the security fabric for posture enforcement.

NEW QUESTION: 18
Which two statements about FortiSASE Geofencing with regional compliance are true? (Choose two answers)
A. You can configure regional compliance on the security POP or the on-premises device, not both.1
B. If no regional compliance rule is configured, the connection is made to the closest security POP.
C. A regional compliance rule can connect only to an on-premises device or only to a security POP.2
D. The connection order for a regional compliance rule is always the security POP first, followed by the on-premises device.

Answer: (SHOW ANSWER)
FortiSASE Geofencing and Regional Compliance allow administrators to control where remote users connect based on their physical location, which is determined by the endpoint's public IP address.3
* Default Connection Behavior: By default, FortiSASE uses a "best-effort" geolocation logic to ensure the lowest latency for the user. If an administrator has not configured a specific regional compliance rule for a user's country or region, FortiClient will automatically attempt to connect to the closest available FortiSASE security PoP (Point of Presence) based on proximity.4
* Regional Compliance Rules: When an organization must enforce data residency or specific security routing requirements, they create Regional Compliance rules. According to the FortiSASE 25 Feature Administration Guide, these rules allow the administrator to override the default "closest PoP" behavior for specific countries.
* Connectivity Options: Within a regional compliance rule, the administrator must specify the destination for the traffic. The system provides a choice between two distinct connection types: a FortiSASE Security PoP or an On-premises device (such as a FortiGate acting as a gateway).5 The documentation specifies that a rule is designed to point to one of these types at a time to satisfy the compliance requirement for that specific region.
* Connection Priority: While multiple connections can be managed in a priority table, the logic for Regional Compliance is focused on directing the user to the designated compliant entry point. Option D is incorrect because the connection order is determined by the Priority and custom fail-over connections table; an administrator can manually adjust the sequence, so it is not "always" the security PoP first.

NEW QUESTION: 19
Refer to the exhibits.

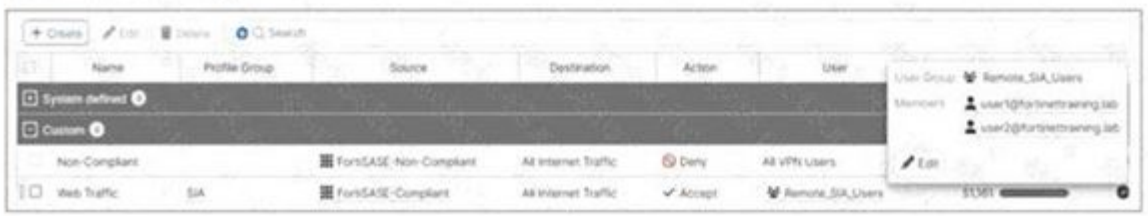
Managed Endpoints

Endpoint	ZTNA Tags (Detailed)	Management Connection	Software OS	FortiClient Version
Jumpbox	FortiSASE-Compliant	Online	Microsoft Windows 11 Professional Edition, 64-bit (build 26100)	7.2.8.1140
Windows-AD	FortiSASE-Compliant FortiSASE-Non-Compliant	Online	Microsoft Windows Server 2019 Datacenter Edition, 64-bit (build 17763)	7.2.6.1076

ZTNA Tagging Rules



Secure Internet Access Policy



freecram.net

Jumpbox and Windows-AD are endpoints from the same remote location. Jumpbox can access the internet through FortiSASE, while Windows-AD can no longer access the internet. Based on the information in the exhibits, which reason explains the outage on Windows-AD? (Choose one answer)

A. The device security posture for Windows-AD has changed.

B. The FortiClient version installed on Windows-AD does not match the expected version on FortiSASE.

C. Windows-AD is excluded from FortiSASE management.

D. The remote VPN user on Windows-AD no longer matches any VPN policy.

Answer: (SHOW ANSWER)

In FortiSASE, Zero Trust Network Access (ZTNA) tags-also known as security posture tags-are used to dynamically grant or deny access based on the real-time security state of an endpoint. This mechanism ensures that only devices meeting specific compliance requirements can access protected resources or the internet.

* Endpoint Analysis: The Managed Endpoints exhibit shows that while Jumpbox only has the FortiSASE-Compliant tag, the Windows-AD endpoint has been assigned both FortiSASE-Compliant and FortiSASE-Non-Compliant tags. This indicates that a security posture check on the Windows-AD device has failed, triggering a rule that applies the non-compliant tag.

* Policy Evaluation: The Secure Internet Access Policy table shows two custom policies. The first policy, named Non-compliant , uses the FortiSASE-Non-Compliant tag as its source and has the action set to Deny . The second policy, Web Traffic , allows access for FortiSASE-Compliant users.

* Root Cause of Outage: Because FortiSASE (powered by FortiOS) processes security policies in a top- down sequence, the " Non-compliant " policy is evaluated first. Since Windows-AD matches the source criteria for this " Deny " policy, its traffic is blocked before it can reach the " Accept " policy.

Although the exhibit shows a warning icon for the FortiClient version on Windows-AD, the direct cause of the internet outage is the explicit Deny policy triggered by the change in the device ' s security posture (the application of the Non-Compliant tag).

NEW QUESTION: 20

Which authentication method overrides any other previously configured user authentication on FortiSASE?

Freecram.net

A. Local

B. SSO

C. RADIUS

D. MFA

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From FortiSASE 24.x/25.x, FortiOS 7.4, FortiAuthenticator 6.5, FortiClient 7.0 and later Exact Extract study guide:

In FortiSASE environments, Single Sign-On (SSO) is prioritized as the primary enterprise authentication mechanism. According to the FortiSASE Configuration Guide and Security Operations documentation, when you configure SAML SSO (Single Sign-On), it serves as a global authentication setting that overrides any previously configured local or remote (RADIUS/LDAP) user authentication methods for the secure web gateway (SWG) and VPN tunnels.

The architectural logic is designed to ensure a seamless " Zero Trust " identity provider (IdP) experience.

Once SSO is enabled and configured (typically using Azure AD, Okta, or FortiAuthenticator as the IdP), FortiSASE redirects authentication requests to the defined IdP. This effectively supersedes manual local user databases or legacy RADIUS configurations to maintain a single source of truth for identity management.

While MFA is often a component of the authentication process, it is a secondary factor, whereas SSO is the foundational method that dictates the authentication flow and overrides prior settings.

NEW QUESTION: 21
What are two benefits of deploying secure private access (SPA) with SD-WAN? (Choose two answers)
A. ZTNA posture check performed by the hub FortiGate
B. Support of both TCP and UDP applications
C. A direct access proxy tunnel from FortiClient to the on-premises FortiGate
D. Inline security inspection by FortiSASE
Answer: (SHOW ANSWER)
According to the NSE7 SASE Enterprise Guide (Pages 46 & 61), deploying Secure Private Access (SPA) with SD-WAN provides advanced security and networking capabilities by routing traffic through global Points of Presence (PoPs).
* Inline Security Inspection (D): A major advantage of this approach is that traffic is routed through FortiSASE PoPs before it reaches private applications. This enables inline security inspection, providing robust protection against threats by applying the full SASE security stack-including antivirus, intrusion prevention, and deep packet inspection-to private access traffic.
* Support for TCP and UDP (B): Organizations with existing FortiGate SD-WAN deployments benefit from broader and seamless access to privately hosted applications. The SD-WAN SPA use case explicitly supports both TCP- and UDP-based applications, ensuring that legacy or specialized services that rely on UDP function correctly over the secure tunnel.
* SD-WAN Optimization: This method leverages the benefits of SD-WAN to optimize traffic flow between the SASE PoP and the corporate SD-WAN hub or data center FortiGate. It is particularly useful for mission-critical applications that require an extra layer of security combined with path optimization.
* Architecture: In this configuration, the FortiSASE Security PoPs act as spokes in the organization's SD-WAN network, relying on IPsec VPN overlays and BGP for secure dynamic routing.
While ZTNA posture checks are a feature of the broader ecosystem, the NSE7 Guide specifically highlights inline inspection and application support (TCP/UDP) as primary advantages of the SD-WAN integrated SPA approach.

NEW QUESTION: 22
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: (SHOW ANSWER)
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.
References:
FortiOS 7.6 Administration Guide: Provides detailed information on ZTNA and its role in ensuring least- privileged access.
FortiSASE 23.2 Documentation: Explains the implementation and benefits of ZTNA within the FortiSASE environment.

NEW QUESTION: 23
Refer to the exhibits.

Traffic logs

Log Details

Details | Security

Web Filter With Inline-CASB

Category	50
Category Description	Information and Computer Security
Direction	outgoing
Event Type	ftgd_allow
Hostname	www.eicar.org
Message	URL belongs to an allowed category in policy
Profile Group	Default (Internet Access)
Request Type	direct
Source Domain	trainingAD.training.lab
Sub Type	webfilter
Type	utm
Timezone	+0000
Unauthenticated User Source	forticlient
URL	https://www.eicar.org/

Application Control With Inline-CASB

Direction	incoming
Event Type	signature
Hostname	www.eicar.org
Incident Serial No.	36709018
Message	Web.Client: HTTPS.BROWSER
Source Domain	trainingAD.training.lab
Sub Type	app-ctrl
Type	utm
Timezone	+0000
Unauthenticated User Source	forticlient
URL	/

Security profile group

FORTINET®
freecram.net



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.
Which configuration on FortiSASE is allowing users to perform the download? (Choose one answer)

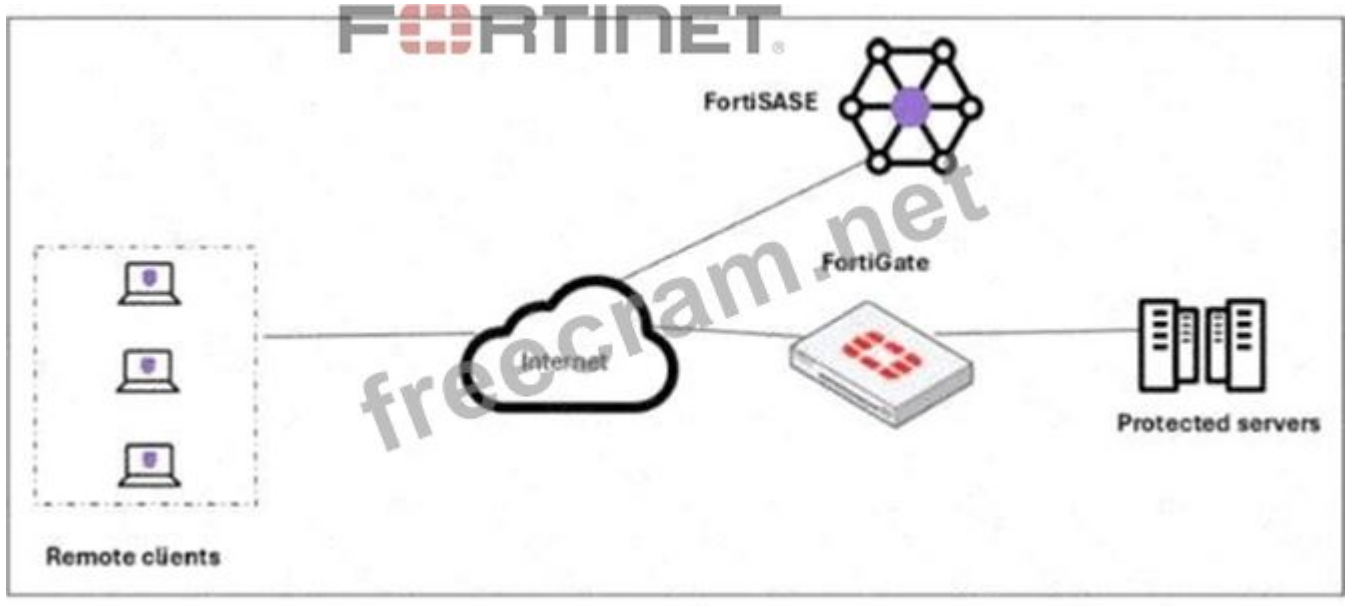
A. Deep inspection is not enabled.
B. Application control is exempting all the browser traffic.
C. Web filter is allowing the URL.
D. Intrusion prevention is disabled.

Answer: (SHOW ANSWER)

The core of the issue shown in the exhibits is the lack of visibility into encrypted traffic.
* HTTPS Encryption: The eicar.org website uses the HTTPS protocol for its downloads. This means the data payload, including the test malware file, is encrypted as it traverses the network.
* SSL Inspection Modes: As seen in the Security profile group exhibit (image_5705fc.jpg), the SSL inspection mode is explicitly set to Certificate inspection mode .
* Visibility Gap: Certificate inspection only analyzes the initial SSL handshake, such as the server certificate and SNI (Server Name Indication). It does not decrypt the traffic payload. Consequently, the antivirus engine in FortiSASE cannot " see " or scan the eicar.com-zip file hidden within the encrypted session.
* Resolution Requirement: To detect and block malicious files over HTTPS, SSL Deep Inspection must be enabled. Deep inspection allows FortiSASE to act as a proxy, decrypting the traffic for full content scanning by the antivirus and IPS engines before re-encrypting it for the endpoint.
* Log Analysis: While the web filtering logs (image_5704e5.jpg) show the traffic is " Allowed " because the URL is not blocked by a web filter category, this is only the first step of inspection. The antivirus engine is present but ineffective because it is blind to the encrypted content due to the lack of deep inspection.

NEW QUESTION: 24

A customer needs to implement device posture checks for their remote endpoints while accessing the protected server. They also want the TCP traffic between the remote endpoints and the protected servers to be processed by FortiGate.



In this scenario, which two setups will achieve these requirements? (Choose two answers)

A. Configure ZTNA tags on FortiGate.
B. Configure FortiGate as a zero trust network access (ZTNA) access proxy.

C. Configure ZTNA servers and ZTNA policies on FortiGate.

D. Configure private access policies on FortiSASE with ZTNA.

Answer: (SHOW ANSWER)

To implement Zero Trust Network Access (ZTNA) where a FortiGate hub enforces device posture and processes traffic directly, specific architectural and configuration steps are required on the FortiGate appliance.
* ZTNA Access Proxy (B): The FortiGate must be configured as a ZTNA access proxy . In this role, the FortiGate acts as a secure gateway that mediates connections between remote users and internal applications. This setup ensures that all TCP traffic is intercepted and processed by the FortiGate, providing a direct, shortest-path connection that bypasses the FortiSASE cloud PoPs for the data plane.
* ZTNA Servers and Policies (C): Within the FortiGate configuration, administrators must define ZTNA servers (which identify the protected applications or resources) and ZTNA policies . ZTNA policies are the enforcement rules that check for valid client certificates and specific ZTNA tags (synchronized from FortiSASE) before allowing access to a resource. This configuration allows the FortiGate to perform continuous posture checks on every session.
* Posture Check Mechanism: While ZTNA tags are used, they are generally synchronized from the FortiSASE Endpoint Management Service (EMS) rather than manually configured on the FortiGate itself. This synchronization ensures the FortiGate has real-time visibility into the security posture (e.g., AV compliance, OS version) of the endpoints as reported by FortiClient.
* Analysis of Incorrect Options:
* Option A: Creating ZTNA tags manually on a FortiGate is technically possible but is not the recommended " setup " in a FortiSASE deployment, as tags are meant to be dynamically assigned by EMS and synced to the fabric.
* Option D: " Private access policies on FortiSASE " refers to the SD-WAN Secure Private Access (SPA) use case. In the SD-WAN SPA model, traffic is steered through the FortiSASE PoP first, whereas the requirement specifically asks for TCP traffic to be processed by the FortiGate using ZTNA.

NEW QUESTION: 25
What happens to the logs on FortiSASE that are older than the configured log retention period? (Choose one answer)

A. The logs are deleted from FortiSASE.1
B. The logs are compressed and archived.
C. The logs are backed up on FortiCloud.
D. The logs are indexed and can be stored in a SQL database.
Answer: (SHOW ANSWER)
In a FortiSASE environment, log management is governed by a cloud-native storage policy that prioritizes performance and resource availability.
* Retention Policy Framework: All FortiSASE instances come with log retention enabled by default.
The standard log retention period is 30 days, though administrators can customize this policy to any duration between 2 and 30 days. This policy applies across all log types, including traffic, security, and event logs.
* Automatic Deletion (A): When logs exceed the configured retention threshold, FortiSASE automatically deletes the older logs from the platform.2 This automatic purging is necessary to free up storage space on the cloud infrastructure and maintain compliance with the organization's data lifecycle settings.
* Persistence and Recovery: Once logs are deleted due to the expiration of the retention period, they are generally unrecoverable from the FortiSASE platform.
* Long-Term Storage Solutions: Because FortiSASE is not designed as a long-term archival solution, customers who need to store logs for months or years for regulatory compliance should configure log forwarding to an external server, such as a FortiAnalyzer or a remote Syslog server.
* Analysis of Incorrect Options: * Option B and D: While traditional FortiAnalyzer deployments use SQL indexing and separate "Archive" (raw/compressed) vs. "Analytics" (SQL) tiers, FortiSASE uses a simplified cloud storage model where data is purged rather than archived or tier-shifted upon expiry.
* Option C: While FortiSASE is part of the FortiCloud ecosystem, it does not automatically "back up" expired logs to another FortiCloud service; the deletion is final unless external forwarding is active.

NEW QUESTION: 26
What can be configured on FortiSASE as an additional layer of security for FortiClient registration? (Choose one answer)
A. Security posture tags
B. User verification
C. Device identification1
D. Application inventory
Answer: (SHOW ANSWER)
In a default FortiSASE deployment, endpoints are typically onboarded using a shared invitation code sent via email. While this code simplifies deployment, it can represent a security risk if the code is leaked or intercepted, as any device with the code could potentially register with the SASE management service.
* User Verification (SAML SSO): To mitigate this risk, administrators can enable user verification as an additional layer of security. 3 When this feature is enforced, entering the invitation code is no longer sufficient to complete registration.
* Authentication Workflow: After the end user enters the invitation code in FortiClient, they are prompted to provide their corporate credentials via a SAML SSO login. 5 FortiSASE acts as the Service Provider (SP), while an external identity provider (IdP) such as Microsoft Entra ID, Okta, or FortiAuthenticator verifies the user ' s identity.
* Security Benefit: This ensures that only authenticated users -not just anyone with a valid code-can successfully register an endpoint and receive the organization ' s security and VPN profiles. It prevents unauthorized " shadow " endpoints from joining the managed environment.

* Incorrect Options:
* Option A: Security posture tags are used after registration to determine if an endpoint is compliant (e.g., checking if an antivirus is active); they do not secure the registration process itself.
* Option C and D: Device identification and application inventory are monitoring and visibility features that occur once the endpoint is already managed.
Refer to the exhibit. Based on the configuration shown in image_595357.jpg , FortiSASE will process sessions requiring FortiSandbox inspection in the following two ways:
A). Only endpoints assigned a profile for sandbox detection will be processed by the sandbox feature.
C). All files executed on a USB drive will be sent to FortiSandbox for analysis.
The provided exhibit displays an Endpoint Profile configuration specifically for the Sandbox module. This profile controls how the FortiClient agent on remote endpoints interacts with the integrated FortiSASE cloud sandbox engine.
* Profile Assignment (A): In the FortiSASE architecture, security and endpoint settings are organized into profiles that must be explicitly assigned to users or user groups via endpoint policies.
Consequently, the sandbox detection and remediation features are active only on those endpoints that have been assigned this specific endpoint profile . If an endpoint is not assigned a profile with sandbox enabled, it will not submit files for analysis.
* Removable Media Analysis (C): Under the File Submission Options , the toggle for All Files Executed from Removable Media is enabled (shown in blue). Since USB drives are the most common form of removable media, this configuration ensures that any file executed from a USB drive is intercepted by FortiClient and submitted to the FortiSASE sandbox for behavioral analysis before being allowed to run, protecting the endpoint from offline-delivered threats.
* Understanding Verdict Levels (B): The exhibit shows the Action is set to Quarantine and the Sandbox Detection Verdict Level is set to Medium . This configuration functions as a threshold; FortiClient will quarantine any file that receives a verdict of Medium or higher (including High and Malicious). Option B is incorrect because it claims only medium-level files are quarantined, which ignores the high-risk and malicious files that would also be blocked.
* Sandbox Mode (D): The Sandbox Mode is clearly set to FortiSASE , which utilizes the built-in cloud- native sandbox. This contradicts Option D, which suggests the use of an on-premises or standalone sandbox appliance.

NEW QUESTION: 27
What are the two key features and benefits of Fortinet SOCaaS when integrated with FortiSASE? (Choose two answers)
A. Fortinet SOCaaS offers monitoring only during standard business hours, uses AI without human analysis, and provides annual reports without dashboards or FortiSASE integration.
B. Fortinet SOCaaS monitors only remote users, does not support log forwarding, and provides threat notifications without response guidance or expert meetings.
C. Fortinet SOCaaS allows for consistent security monitoring through log forwarding, offers rapid threat notifications and response guidance, and includes intuitive dashboards.
D. Fortinet SOCaaS provides 24x7x365 cloud-based monitoring by Fortinet experts using AI, machine learning, and human analysis.
E. Fortinet SOCaaS is a standalone service that monitors only FortiGate environments, provides automated patching without human analysis, and does not integrate with FortiSASE.
Answer: (SHOW ANSWER)
Integrating Fortinet SOCaaS (Security Operations Center as a Service) with FortiSASE provides a managed extension of your security team, combining automated AI/ML-driven triage with human expertise to secure remote and on-premises users.
* Consistent Security Monitoring and Dashboards (C): Fortinet SOCaaS ensures that your security posture remains robust through

seamless integration. This is achieved by configuring FortiSASE to forward pertinent security logs to the SOCaaS cloud, ensuring that analysts have the necessary data to detect anomalies across your network. The service provides verified threat notifications with detailed response guidance and mitigation recommendations. Furthermore, a built-in portal offers intuitive dashboards to track threats and manage escalated alerts.
* 24x7x365 Expert-Led Monitoring (D): This feature addresses the cybersecurity skills gap by providing around-the-clock vigilance. A global team of Fortinet Security Analysts works 24x7x365 to monitor logs and investigate events. The platform leverages AI and Machine Learning for automated alert triage, while human experts perform in-depth analysis to eliminate false positives and validate threats.
* Operational Efficiency: By offloading tedious manual work and triage to Fortinet experts, your internal security team can reduce burnout and focus on higher-value tasks while maintaining a superior security posture for both SASE and on-premises environments.

NEW QUESTION: 28
What are the key differences between the FortiSASE BGP per overlay and BGP on loopback routing design methods? (Choose one answer)
A. BGP per overlay can use separate iBGP sessions for each spoke-to-hub tunnel with mode-cfg enabled for IP address assignment, while BGP on loopback uses a single iBGP session per hub terminating on a loopback interface to simplify configuration and reduce advertised routes.
B. BGP per overlay establishes a single iBGP session per hub on a loopback interface, while BGP on loopback requires mode-cfg for IP address assignment and uses multiple iBGP sessions per tunnel.
C. BGP per overlay is used for loopback interfaces to reduce routes, while BGP on loopback is the default method requiring separate iBGP sessions for each spoke.
D. BGP per overlay simplifies hub configuration without mode-cfg, while BGP on loopback establishes multiple iBGP sessions for each tunnel to increase advertised routes.
Answer: (SHOW ANSWER)
FortiSASE supports two main routing design methods for Secure Private Access (SPA) when connecting to a FortiGate SD-WAN hub:
* BGP per Overlay (Traditional/Default Method): In this configuration, a separate iBGP session is established over every individual IPsec overlay (tunnel) between the FortiSASE PoP and the hub. These sessions terminate on the tunnel interface IP addresses. To facilitate this, the hubs typically use the IPsec VPN mode-cfg feature to dynamically assign tunnel IP addresses to the SASE PoPs. For every LAN prefix, the system generates multiple BGP routes-one for each overlay-which increases the total number of routes advertised across the network.
* BGP on Loopback (Modern Alternative): This newer design establishes only a single iBGP session between the spoke and the hub, regardless of how many physical or logical overlays (tunnels) connect them. The session is terminated on a loopback interface on both sides.
* Key Advantages of BGP on Loopback:
* Reduced Complexity: It significantly simplifies the BGP configuration because there are fewer neighbors to manage.2
* Improved Scalability: It greatly reduces the volume of routes advertised, as only a single BGP route is generated for each LAN prefix, making it the preferred choice for large-scale deployments.
* Resiliency: The BGP session remains active as long as the loopback is reachable via any of the available overlays, meaning no BGP convergence is required if a single overlay fails.

NEW QUESTION: 29
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: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 30
When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)
Freecram.net
A. Vulnerability scan
B. SSL inspection
C. Anti-ransomware protection
D. Web filter
E. ZTNA tags
Answer: (SHOW ANSWER)
When deploying FortiSASE agent-based clients, several features are available that are not typically available with an agentless solution. These features enhance the security and management capabilities for endpoints.
* Vulnerability Scan:
* Agent-based clients can perform vulnerability scans on endpoints to identify and remediate security weaknesses.
* This proactive approach helps to ensure that endpoints are secure and compliant with security policies.
* SSL Inspection:
* Agent-based clients can perform SSL inspection to decrypt and inspect encrypted traffic for threats.
* This feature is critical for detecting malicious activities hidden within SSL/TLS encrypted traffic.
* Web Filter:
* Web filtering is a key feature available with agent-based clients, allowing administrators to control and monitor web access.
* This feature helps enforce acceptable use policies and protect users from web-based threats.
References:
FortiOS 7.6 Administration Guide: Explains the features and benefits of deploying agent-based clients.
FortiSASE 23.2 Documentation: Details the differences between agent-based and agentless solutions and the additional features provided by agent-based deployments.

NEW QUESTION: 31

When configuring the DLP rule in FortiSASE using Regex format, what would be the correct order for the configuration steps? (Place the four correct steps in order)



Answer:



Explanation:

1. DLP Data Pattern
2. DLP Dictionary
3. DLP Sensor
4. DLP Profile

The FortiSASE Data Loss Prevention (DLP) framework follows a hierarchical object-oriented structure.

When creating a custom DLP rule using Regular Expressions (Regex), the administrator must build the components from the most granular level upward to the policy level.

* DLP Data Pattern: This is the first step where the actual Regex string is defined. The pattern specifies what specific data string (e.g., a specific credit card format or employee ID) the engine should look for.
* DLP Dictionary: Once the pattern is created, it must be added to a Dictionary. The dictionary acts as a container that groups one or more data patterns together for easier management.

* DLP Sensor: The dictionary is then linked to a DLP Sensor. Within the sensor, you define the "Rule" which specifies the dictionary to use and the action to take (such as block, log, or quarantine) when a match occurs.
* DLP Profile: Finally, the sensor is applied to a DLP Profile. This profile is the high-level object that is ultimately selected within a FortiSASE Security Policy to inspect traffic for sensitive data.

Valid NSE7_SSE_AD-25 Dumps shared by ExamDiscuss.com for Helping Passing NSE7_SSE_AD-25 Exam! ExamDiscuss.com now offer the **newest NSE7_SSE_AD-25 exam dumps**, the ExamDiscuss.com NSE7_SSE_AD-25 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com NSE7_SSE_AD-25 dumps with Test Engine here: https://www.examdiscuss.com/Fortinet/exam/NSE7_SSE_AD-25/premium/ (**109** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
A customer wants to ensure secure access to private applications for their users by replacing their VPN.
Which two SASE technologies can you use to accomplish this task? (Choose two answers)
A. Secure web gateway (SWG) and cloud access security broker (CASB)
B. SD-WAN on-ramp
C. Secure SD-WAN
D. Zero trust network access (ZTNA)
Answer: (SHOW ANSWER)
The correct answers are C. Secure SD-WAN and D. Zero trust network access (ZTNA) . In FortiSASE, secure access to private applications is part of Secure Private Access (SPA) . The study guide identifies ZTNA as the SASE technology that provides "secure, explicit, identity-based access," and explains that applying ZTNA shifts implicit access to explicit control by combining user authentication, continuous identity, context validation, and integration. This directly supports replacing traditional VPN access for private applications.
The guide also states that organizations can integrate FortiSASE with existing FortiGate SD-WAN deployments "to provide remote users access to private resources," where FortiSASE security POPs act as spokes to the FortiGate SD-WAN hub. In the SPA section, FortiSASE private access is described as using ZTNA and SD-WAN integration for secure cloud and data center application access. SWG and CASB are not the best answers because SWG is for secure internet/web access, while CASB focuses on SaaS visibility and data protection, not private application VPN replacement. SD-WAN on-ramp is a deployment method, not the core SASE technology pair asked for here.

NEW QUESTION: 33
Which statement about FortiSASE and SAML is true? (Choose one answer)
A. FortiSASE acts as the SP, relies on an external IdP, and can use SAML group matching.
B. FortiSASE supports SAML login but cannot use SAML group matching.
C. FortiSASE acts as the IdP and can perform SAML group matching internally.
D. FortiSASE includes IdP functionality and uses it for SAML group matching.
Answer: (SHOW ANSWER)
FortiSASE utilizes Security Assertion Markup Language (SAML) to provide a seamless Single Sign-On (SSO) experience for remote users connecting to the cloud infrastructure.
* Role Identification: In a SAML exchange, FortiSASE functions as the Service Provider (SP) . It relies on an external Identity Provider (IdP)

-such as Microsoft Entra ID (formerly Azure AD), Okta, or FortiAuthenticator-to authenticate the user ' s identity and provide security assertions. 2
* SAML Group Matching: One of the core features of the FortiSASE SAML implementation is the ability to perform group matching . During the authentication process, the IdP sends a SAML assertion that typically includes an " Attribute Statement " containing the user ' s group memberships. 3 FortiSASE captures this attribute and matches it against locally defined SAML user groups.
* Policy Enforcement: This group matching capability is critical because it allows administrators to apply different Security Internet Access (SIA) or Secure Private Access (SPA) policies based on the user ' s role (e.g., " Marketing " vs. " Finance ") rather than managing individual users manually.
* Analysis of Incorrect Options: * Options C and D are incorrect because FortiSASE does not natively act as a SAML IdP; it is designed to consume assertions from professional identity management platforms.
* Option B is incorrect because FortiSASE fully supports and relies upon group matching for enterprise-scale policy management.

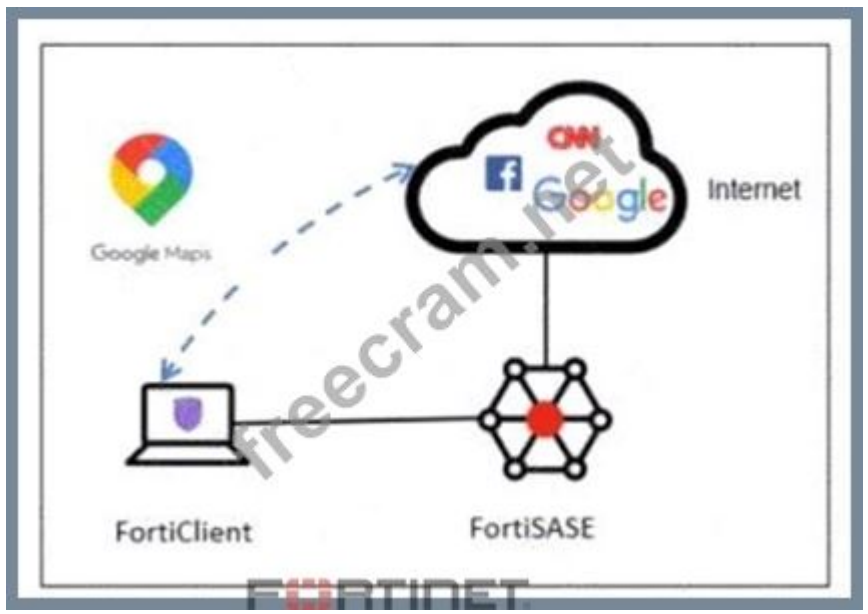
NEW QUESTION: 34
How does FortiSASE address the market trends of multicloud and Software-as-a-Service (SaaS) adoption, hybrid workforce, and zero trust? (Choose one answer)
A. It focuses solely on securing on-premises networks, ignoring cloud and remote work challenges.
B. It prioritizes legacy VPN connections for hybrid workforces, bypassing modern cloud and zero-trust security measures.
C. It provides visibility and control for multicloud and SaaS environments, ensures secure and seamless access for hybrid workforces, and implements zero-trust principles.1
D. It supports only zero-trust frameworks without addressing multicloud or hybrid workforce needs.
Answer: (SHOW ANSWER)
FortiSASE is designed as a unified, single-vendor solution that specifically targets the convergence of networking and security to address the modern challenges of a distributed enterprise. 2
* Multicloud and SaaS Adoption: FortiSASE addresses the surge in cloud-first strategies by providing Next-Generation Dual-Mode CASB (Cloud Access Security Broker). 3 This feature uses both inline and API-based inspection to provide comprehensive visibility into sanctioned and unsanctioned SaaS applications (Shadow IT), ensuring that data is protected regardless of whether it resides in AWS, Azure, Google Cloud, or SaaS platforms like Microsoft 365.
* Hybrid Workforce: To support a workforce that moves between the home, the office, and public spaces, FortiSASE delivers consistent security posture . 5 It replaces the inconsistent experience of legacy VPNs with a geographically dispersed network of over 150 Points of Presence (PoPs), ensuring low-latency access to applications while maintaining high-performance SSL inspection and threat detection for all remote users.
* Zero Trust Integration: Central to the FortiSASE architecture is Universal ZTNA (Zero Trust Network Access). 7 Unlike traditional VPNs that grant broad network access, ZTNA applies the principle of " never trust, always verify " . It grants access on a per-session, per-application basis, continuously verifying the device posture and user identity before and during application access. 9 This shift from implicit to explicit trust significantly reduces the internal attack surface and mitigates the risk of lateral movement by attackers.
By integrating these components into a single operating system (FortiOS) and managed via a single console, FortiSASE simplifies IT operations while delivering the visibility and control required for today ' s multicloud and hybrid environments.

NEW QUESTION: 35
What is the maximum number of Secure Private Access (SPA) service connections (SPA hubs) supported in the SPA use case? (Choose one answer)

A. 8
B. 12
C. 4
D. 16
Answer: (SHOW ANSWER)
In recent versions of FortiSASE (starting from version 24.4 and later), the platform has increased its scalability to support larger enterprise environments.
* Maximum Hub Support : According to the FortiSASE Mature Administration Guide and the FortiSASE 25.3.148 Feature Release Notes , administrators can now configure a maximum of 12 SPA Service Connections (SPA hubs) . Previously, this limit was restricted to 4 hubs.
* Scalability for Large Enterprises : This enhancement allows organizations with complex, geographically dispersed networks-such as those with multiple regional datacenters or cloud hubs-to integrate up to 12 distinct FortiGate SD-WAN hubs into their SASE infrastructure.
* Service Connection Licensing : Each SPA hub requires a dedicated FortiGate SPA Service Connection license . In MSSP environments using FortiCloud Organizations, a single FortiSASE instance can inherit these licenses from a root OU, supporting up to the same cumulative maximum of
12 service connections.
* Routing and Performance : These 12 hubs form the " Private Access " backbone, where FortiSASE security PoPs act as spokes. The use of BGP (either per-overlay or on loopback) ensures that traffic is dynamically routed to the optimal hub based on the destination network and defined SLA priorities.

NEW QUESTION: 36
An organization must block user attempts to log in to non-company resources while using Microsoft Office 365 to prevent users from accessing unapproved cloud resources. Which FortiSASE feature can you implement to meet this requirement? (Choose one answer)
A. Data loss prevention (DLP) with Microsoft Purview Information Protection (MPIP)
B. DNS filter with domain filter
C. Application control with inline-CASB
D. Web filter with inline-CASB
Answer: (SHOW ANSWER)
The correct answer is D. Web filter with inline-CASB . The FortiSASE study guide states that FortiCASB provides cloud-based and API-based capabilities for deep inspection of SaaS applications, enabling monitoring, analysis, and reporting. It also states that FortiSASE provides inline CASB functionality with a web filter and application control security features , while DLP protects data at rest and in motion. This question specifically describes restricting Microsoft Office 365 access by tenant, meaning users should be allowed to access company-approved Microsoft 365 resources but blocked from logging in to non-company or personal resources. Fortinet's FortiSASE documentation describes this exact use case as "restricted SaaS access," where organizations restrict access to Microsoft Office 365, Google Workspace, and similar SaaS services by tenant to block non-company login attempts and prevent access to non-approved cloud resources. Fortinet's Office 365 example confirms this is implemented through FortiSASE Web Filter with Inline-CASB, using inline-CASB headers to allow corporate domains and deny personal accounts.

NEW QUESTION: 37
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.
Answer: (SHOW ANSWER)
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.
References:
FortiOS 7.6 Administration Guide: Provides details on split tunneling configuration.
FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

NEW QUESTION: 38
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: (SHOW ANSWER)
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.
References:
FortiOS 7.6 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.

NEW QUESTION: 39
You are configuring FortiSASE SSL deep inspection. What is required for FortiSASE to inspect encrypted traffic? (Choose one answer)
A. FortiSASE uses a third-party CA certificate without importing it to client machines, and SSL deep inspection supports only web filtering and application control.
B. FortiSASE acts as a root CA without needing a certificate, and SSL deep inspection is used only for split DNS and video filtering.
C. FortiSASE requires an external CA to issue certificates to client machines, and SSL deep inspection supports only antivirus and file filter.
D. FortiSASE acts as a certificate authority (CA) with a self-signed or internal CA certificate, requiring the root CA certificate to be imported into client machines.
Answer: (SHOW ANSWER)
SSL deep inspection (DPI) is a critical security function that allows FortiSASE to decrypt and inspect the actual payload of encrypted traffic (such as HTTPS, SMTPS, and FTPS) to identify and block hidden threats.
* The Role of the CA: For this process to occur, FortiSASE must act as a " man-in-the-middle " by intercepting the SSL session, decrypting it for inspection, and then re-encrypting it before sending it to the endpoint. 2 To re-encrypt the traffic, FortiSASE acts as a Certificate Authority (CA) and signs a new certificate for the destination website on the fly.
* Certificate Types: This CA role can be fulfilled using the default self-signed certificate provided by Fortinet (typically Fortinet_CA_SSL) or a certificate issued by an organization ' s internal/private CA
. Publicly trusted third-party CAs (like DigiCert or Let ' s Encrypt) do not sell CA-capable certificates that can be used for this type of inspection.
* Client Machine Requirement: Because the endpoint's browser or operating system will not natively trust a certificate signed by a private or self-signed CA, the root CA certificate must be imported into the Trusted Root Certification Authorities store on all managed client machines. Failure to do so results in persistent certificate warnings or blocked connections for the end user.
* Supported Features: Once enabled, SSL deep inspection provides the necessary visibility for high- level security features to function,

including Antivirus , Web Filtering , Data Loss Prevention (DLP)
, File Filter , and Application Control .

Valid NSE7_SSE_AD-25 Dumps shared by ExamDiscuss.com for Helping Passing NSE7_SSE_AD-25 Exam! ExamDiscuss.com now offer the **newest NSE7_SSE_AD-25 exam dumps**, the ExamDiscuss.com NSE7_SSE_AD-25 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com NSE7_SSE_AD-25 dumps with Test Engine here: https://www.examdiscuss.com/Fortinet/exam/NSE7_SSE_AD-25/premium/ (**109** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)