PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7FortiSASE 25 Enterprise Administrator

Fortinet NSE7_SSE_AD-25

Version Demo

Total Demo Questions: 10

Total Premium Questions: 108

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSASE architecture	8
Topic 2, FortiSASE deployment	32
Topic 3, Secure Internet Access	10
Topic 4, Secure Private Access	27
Topic 5, Secure Web Access	3
Topic 6, Data protection	7
Topic 7, SaaS security	8
Topic 8, Monitoring and troubleshooting	12
Topic 9, Mix Questions	1
Total	108

QUESTION NO: 1 - (DRAG DROP)

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:

For a Regex-based DLP configuration, build the objects in dependency order, starting with the item that defines exactly what FortiSASE must detect. Create the **DLP Data Pattern** first. This is the granular matching object in which the administrator enters the regular expression used to recognize sensitive information, such as an organization-specific identifier or another structured data format.

Next, create the **DLP Dictionary**. The dictionary provides the reusable grouping layer for one or more data patterns. Adding the Regex data pattern to a dictionary makes the matching definition available for DLP inspection configuration.

After the dictionary is available, create the **DLP Sensor**. The sensor is where the dictionary is associated with the DLP inspection rule and the resulting handling behavior is configured. In other words, the rule behavior belongs within the sensor configuration rather than being a separate top-level step in this sequence.

Finally, create the **DLP Profile**. The profile is the higher-level configuration that uses the sensor and is selected when applying DLP inspection to the relevant FortiSASE security policy. This bottom-up order ensures every object exists before an object that references it is configured. Fortinet's FortiSASE documentation is available through the FortiSASE documentation portal, and Fortinet's DLP feature documentation provides additional context at Data leak prevention.

QUESTION NO: 2 - (SIMULATION)

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: See the explanation for the answer

Explanation:

Correct configuration order:

First, create the **DLP Data Pattern** and define the regular expression. Add that pattern to a **DLP Dictionary**, then reference the dictionary in a **DLP Sensor** and configure the matching/action behavior. Finally, add the sensor to a **DLP Profile**, which can be applied to the relevant FortiSASE security policy.

DLP Rule is not one of the four objects to place in this configuration sequence.

QUESTION NO: 3

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: B

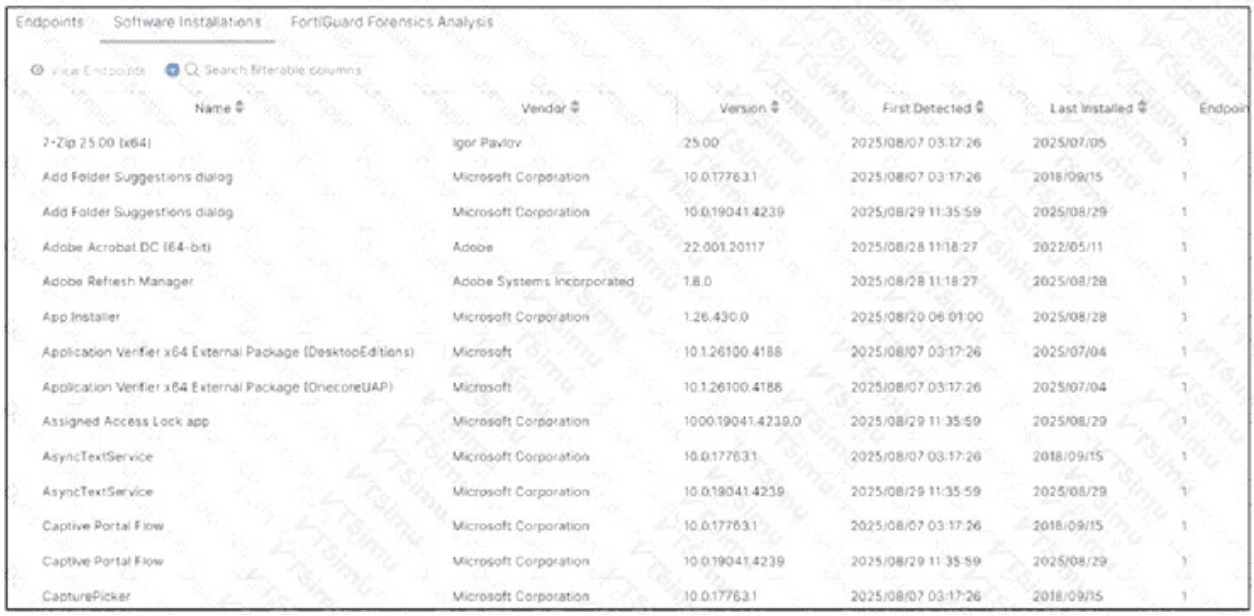
Explanation:

Log allowed traffic is set to Security Events for all policies. is correct because FortiSASE reports are populated from the log data generated by traffic processing and security inspection. The *Log Allowed Traffic* setting controls whether routine traffic that is permitted by a policy is recorded. When every policy is configured to log only *Security Events*, FortiSASE retains events associated with security detections or other security-significant activity, rather than producing logs for the full volume of successfully allowed sessions.

As a result, a daily summary can appear nearly empty in an environment where users primarily access permitted applications and websites without triggering security events. The report reflects the available logs; it does not independently recreate ordinary traffic activity that was not selected for logging. Therefore, the observed lack of report entries is consistent with restrictive allowed-traffic logging across the policy set. Administrators should choose the logging level based on the organization's reporting, troubleshooting, storage, and visibility requirements. Fortinet's FortiSASE documentation describes policy configuration and logging behavior in the FortiSASE Administration Guide. Fortinet also provides reporting and log-analysis guidance through its FortiSASE product documentation.

QUESTION NO: 4

Refer to the exhibit.


Endpoints | Software Installations | FortiGuard Forensics Analysis

View Endpoints | Search filterable columns

Name	Vendor	Version	First Detected	Last Installed	Endpoint
7-Zip 25.00 (x64)	Igor Pavlov	25.00	2025/08/07 03:17:26	2025/07/05	1
Add Folder Suggestions dialog	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
Add Folder Suggestions dialog	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
Adobe Acrobat DC (64-bit)	Adobe	22.001.20117	2025/08/28 11:18:27	2022/05/11	1
Adobe Refresh Manager	Adobe Systems Incorporated	1.8.0	2025/08/28 11:18:27	2025/08/28	1
App Installer	Microsoft Corporation	1.26.430.0	2025/08/20 06:01:00	2025/08/28	1
Application Verifier x64 External Package (DesktopEditions)	Microsoft	10.1.26100.4188	2025/08/07 03:17:26	2025/07/04	1
Application Verifier x64 External Package (OnecoreUAP)	Microsoft	10.1.26100.4188	2025/08/07 03:17:26	2025/07/04	1
Assigned Access Lock app	Microsoft Corporation	1000.19041.4239.0	2025/08/29 11:35:59	2025/08/29	1
AsyncTextService	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
AsyncTextService	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
Captive Portal Flow	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1
Captive Portal Flow	Microsoft Corporation	10.0.19041.4239	2025/08/29 11:35:59	2025/08/29	1
CapturePicker	Microsoft Corporation	10.0.17763.1	2025/08/07 03:17:26	2018/09/15	1

Which type of information or actions are available to a FortiSASE administrator from the following output? (Choose one answer)

A. Administrators can view and configure endpoint profiles and ZTNA tags.

B. Administrators can view and configure automatic patching of endpoints, and first detected date for applications.

C. Administrators can view latest application version available and push updates to managed endpoints.

D. Administrators can view application details, such as vendor, version, and installation dates to identify unwanted or outdated software.

ANSWER: D

Explanation:

Administrators can view application details, such as vendor, version, and installation dates to identify unwanted or outdated software. The exhibit is the Software Installations inventory view, which consolidates software discovered on endpoints managed through the FortiSASE endpoint-management integration. For each detected application, the administrator can review identifying and audit-relevant metadata, including the application name, software vendor, installed version, first-detected time, and last-installed time. This visibility supports endpoint software hygiene and security investigations: an administrator can identify applications that are unauthorized, no longer approved by policy, potentially unwanted, or running versions that warrant further review because of age or known exposure.

The inventory also supports operational scoping by allowing the administrator to pivot to the endpoints on which a selected application is installed. This enables targeted follow-up, such as validating business need, applying an endpoint-control policy, or coordinating remediation with the endpoint owner. Fortinet documents FortiSASE administration and endpoint visibility features in its FortiSASE documentation portal. The related endpoint-management capabilities and software inventory concepts are documented in the FortiClient EMS Administration Guide.

QUESTION NO: 5

An organization is deciding whether to use agent-based or agentless secure internet access for managed employees. The security team requires endpoint-resident protection and endpoint posture information.

Which two capabilities require an agent-based FortiClient deployment? (Choose two answers)

A. Vulnerability scanning

B. Anti-ransomware protection

C. Web filtering

D. SSL deep inspection

ANSWER: A B

Explanation:

Vulnerability scanning and anti-ransomware protection rely on endpoint-resident FortiClient capabilities. They require local visibility into installed software, endpoint activity, and files or processes on the managed device.

Web filtering and SSL inspection can be delivered through FortiSASE for traffic that is steered to the service, including supported agentless SWG deployments. They do not by themselves provide endpoint-resident protection capabilities.

QUESTION NO: 6

Which secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based end points?

A. SIA for inline-CASB users

B. SIA for agentless remote users

C. SIA for SSLVPN remote users

D. SIA for site-based remote users

ANSWER: D

Explanation:

SIA for site-based remote users is correct because the SIA connection is deployed at the site perimeter rather than individually on every endpoint. A FortiGate at the remote site establishes connectivity to the FortiSASE point of presence, typically using an IPsec tunnel, and forwards the site's internet-bound traffic through FortiSASE security inspection. As a result, the FortiGate applies the traffic steering and tunnel configuration once for the location, while user workstations and other devices behind it can access the internet without a FortiClient installation or browser-level explicit proxy configuration. This model is particularly appropriate for branch offices, retail sites, and other locations where many managed or unmanaged devices require consistent secure internet access and centralized enforcement. FortiSASE then applies the organization's configured security controls, such as web filtering and firewall policies, to traffic sent through the site connection. Fortinet documents site-based SIA as a deployment model in which a FortiGate connects a site to FortiSASE, avoiding per-endpoint onboarding for protected site traffic. See the FortiSASE Administration Guide and Fortinet's FortiSASE product documentation overview.

QUESTION NO: 7

An organization has users in several countries and wants to apply regional compliance requirements to FortiSASE endpoint connections.

Which two statements about regional compliance are correct? (Choose two answers)

A. If no regional compliance rule is configured, the endpoint connects to the closest security POP.

B. A regional compliance rule can require an endpoint to connect through both a security POP and an on-premises device.

C. A regional compliance rule can designate either a security POP or an on-premises device as its connection destination.

D. Regional compliance rules replace geofencing deny-list controls.

ANSWER: A C

Explanation:

If no regional compliance rule matches an endpoint connection, FortiSASE normally connects the endpoint to the closest available security POP. This provides the normal latency-optimized connection behavior.

A regional compliance rule can designate either a security POP or an on-premises device as the connection destination for matching endpoints. The rule does not require the endpoint to connect to both destinations in sequence. Geofencing is a separate capability used to allow or deny connections based on geographic origin; it does not define the regional-compliance destination.

QUESTION NO: 8

An organization needs to resolve internal hostnames using its internal rather than public DNS servers for remotely connected endpoints. Which two components must be configured on FortiSASE to achieve this? (Choose two.)

A. SSL deep inspection

B. Split DNS rules

C. Split tunnelling destinations

D. DNS filter

ANSWER: B C

Explanation:

Split DNS rules and **Split tunnelling destinations** work together to provide internal name resolution for remote endpoints. A split DNS rule identifies the organization's internal DNS namespace, such as an internal domain suffix, and associates queries for that namespace with the organization's internal DNS servers. This ensures that lookups for private names are sent to the authoritative internal resolvers instead of being forwarded to public DNS infrastructure. Split DNS therefore supplies the name-based decision and the intended DNS-server selection.

The internal DNS servers must also be reachable through the protected private-access path. Split tunnelling destinations define the private networks or host destinations that remote endpoint traffic must send through the FortiSASE tunnel. Including the internal DNS-server addresses or their reachable network in those destinations ensures that the DNS packets selected by the split DNS rule can traverse the tunnel and reach the internal resolvers. Together, these settings provide both correct DNS query selection and a valid routed path to the internal DNS service. Fortinet documents FortiSASE remote-access and traffic-steering configuration in the FortiSASE Administration Guide; related endpoint VPN and DNS behavior is covered in the FortiClient Administration Guide.

QUESTION NO: 9

An administrator is deploying FortiSASE Branch On-Ramp for a branch that requires resilient connectivity to the FortiSASE service and access to private resources advertised through Secure Private Access (SPA).

Which two statements are correct? (Choose two answers)

A. A branch device can connect to two or more on-ramp locations.

B. Branch On-Ramp uses CAPWAP tunnels to connect to FortiSASE.

C. Branch On-Ramp and SPA share the same BGP configuration.

D. Branch On-Ramp requires the FortiSASE CA certificate to establish its IPsec tunnels.

ANSWER: A C

Explanation:

A branch device can connect to two or more on-ramp locations, which allows the branch deployment to use multiple FortiSASE on-ramp connections for resiliency. Branch On-Ramp uses IKEv2 for its IPsec connectivity.

Branch On-Ramp and SPA share the same BGP configuration, allowing routes for branch networks and private resources to be exchanged consistently. CAPWAP is not the tunnel protocol for Branch On-Ramp, and an endpoint CA certificate is unrelated to establishing the branch IPsec tunnels.

QUESTION NO: 10

What is the purpose of the grace period for off-net endpoints in the FortiSASE Network Lockdown feature? (Choose one answer)

A. To allow users to attempt VPN reconnection before restrictions are applied

B. To bypass security policies for specific applications

C. To permanently block network access for non-compliant endpoints

D. To automatically reset the FortiClient configuration

ANSWER: A

Explanation:

To allow users to attempt VPN reconnection before restrictions are applied is correct because the Network Lockdown grace period is a controlled transition interval for an endpoint that has been detected as off-net. Rather than immediately cutting off connectivity, FortiClient gives the user time to establish the configured FortiSASE VPN tunnel or another approved corporate tunnel. This preserves a practical path for the endpoint to return to a protected, policy-compliant connection state without requiring an administrator to intervene.

Once the endpoint successfully connects through the secure tunnel, its traffic can again be handled by the FortiSASE security services and the device is no longer subject to off-net lockdown enforcement. If a secure connection is not established before the configured interval ends, Network Lockdown applies its connectivity restrictions, while destinations explicitly configured as exemptions can remain reachable. This design supports zero-trust enforcement while accommodating normal events such as a user changing networks, waking a device, or temporarily losing a tunnel connection. Fortinet documents Network Lockdown and endpoint connectivity controls in the FortiSASE Administration Guide; product documentation is also available through the FortiSASE documentation portal.