



Palo Alto Networks NGFW-Engineer Practice Questions

Shared by Vargas on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

Options:

- A- Service graph
- B- Ansible automation modules
- C- Panorama role-based access control (RBAC)
- D- CN-Series firewalls

Answer:

D

Question 2

Question Type: MultipleChoice

Which two actions in the IKE Gateways will allow implementation of post-quantum cryptography when building VPNs between multiple Palo Alto Networks NGFWs? (Choose two.)

Options:

- A- Select IKE v2, enable the Advanced Options * PQ PPK, then set a 64+ character string for the post-quantum pre shared key.
- B- Ensure Authentication is set to "certificate," then import a post-quantum derived certificate.
- C- Select IKE v2 Preferred, enable the Advanced Options * PQ KEM, then add one or more "Rounds."
- D- Select IKE v2, enable the Advanced Options * PQ KEM, then create an IKE Crypto Profile with Advanced Options adding one or more "Rounds."

Answer:

C, D

Explanation:

To implement post-quantum cryptography (PQC) in VPNs between Palo Alto Networks NGFWs, you would enable the PQ KEM (Post-Quantum Key Encapsulation Mechanism) in the IKE gateway configuration. This enables the firewall to use quantum-resistant encryption for key exchange, which is an essential part of securing communications against the potential future threats posed by quantum computing.

By selecting IKE v2 Preferred and enabling the PQ KEM option under Advanced Options, you can add specific Rounds for the post-quantum cryptography process, which will help in implementing quantum-resistant key exchange methods.

This option similarly selects IKE v2 and enables PQ KEM while also creating a dedicated IKE Crypto Profile with the necessary Rounds configured for post-quantum cryptography.



Question 3

Question Type: MultipleChoice

According to dynamic updates best practices, what is the recommended threshold value for content updates in a mission- critical network?

Options:

- A- 8 hours
- B- 16 hours
- C- 32 hours
- D- 48 hours

Answer:

A



Explanation:

For a mission-critical network, it is recommended to configure the content update threshold to 8 hours. This ensures that the network is protected with the latest threat intelligence, updates to signatures, and other critical content, minimizing the exposure to newly discovered vulnerabilities and threats.

Regular content updates are crucial in mission-critical environments to ensure the firewall is up-to-date with the latest protections. 8 hours is considered an optimal balance between timely updates and network performance.

Question 4

Question Type: MultipleChoice

When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

Options:

- A- Service graph
- B- Ansible automation modules
- C- Panorama role-based access control
- D- CN-Series firewalls

P2P
exams

Answer:

D

Explanation:

When integrating Kubernetes with Palo Alto Networks NGFWs, the CN-Series firewalls are specifically designed to secure traffic between microservices in containerized environments. These firewalls provide advanced security features like Application Identification (App-ID), URL filtering, and Threat Prevention to secure communication between containers and microservices within a Kubernetes environment.

Question 5

Question Type: MultipleChoice

What is a result of enabling split tunneling in the GlobalProtect portal configuration with the "Both Network Traffic and DNS" option?

Options:

- A- It specifies when the secondary DNS server is used for resolution to allow access to specific domains that are not managed by the VPN.
- B- It allows users to access internal resources when connected locally and external resources when connected remotely using the same FQDN.
- C- It allows devices on a local network to access blocked websites by changing which DNS

P2P
exams

server resolves certain domain names.

D- It specifies which domains are resolved by the VPN-assigned DNS servers and which domains are resolved by the local DNS servers.

Answer:

D

Explanation:

When split tunneling is enabled with the 'Both Network Traffic and DNS' option in the GlobalProtect portal configuration, it allows the firewall to control which traffic is sent over the VPN tunnel and which is not. Specifically, it determines which domains are resolved by the VPN-assigned DNS servers (for domains requiring VPN access) and which are resolved by local DNS servers (for domains that can be accessed without the VPN tunnel).

Question 6

Question Type: MultipleChoice

A multinational organization wants to use the Cloud Identity Engine (CIE) to aggregate identity data from multiple sources (on premises AD, Azure AD, Okta) while enforcing strict data isolation for different regional business units. Each region's firewalls, managed via Panorama, must only receive the user and group information relevant to that region. The organization aims to minimize administrative overhead while meeting data sovereignty requirements.

Which approach achieves this segmentation of identity data?

Options:

A- Create one CIE tenant, aggregate all identity data into a single view, and redistribute the full dataset to all firewalls. Rely on per-firewall Security policies to restrict access to out-of-scope user and group information.

B- Establish separate CIE tenants for each business unit, integrating each tenant with the relevant identity sources. Redistribute user and group data from each tenant only to the region's firewalls, maintaining a strict one-to-one mapping of tenant to business unit.

C- Disable redistribution of identity data entirely. Instead, configure each regional firewall to pull user and group details directly from its local identity providers (IdPs).

D- Deploy a single CIE tenant that collects all identity data, then configure segments within the tenant to filter and redistribute only the relevant user/group sets to each regional firewall group.

Answer:

B

Explanation:

To meet the requirement of data isolation for different regional business units while minimizing administrative overhead, the best approach is to establish separate Cloud Identity Engine (CIE) tenants for each business unit. Each tenant would be integrated with the relevant identity sources (such as on-premises AD, Azure AD, and Okta) for that specific region. This ensures that the identity data for each region is kept isolated and only relevant user and group data is distributed to the respective regional firewalls.

By maintaining a strict one-to-one mapping between CIE tenants and business units, the organization ensures that each region's firewall only receives the user and group data relevant to that region, thus meeting data sovereignty requirements and minimizing administrative complexity.

Question 7

Question Type: MultipleChoice

Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?

Options:

- A- DDNS
- B- Link Duplex
- C- NetFlow
- D- LLDP

Answer:

C

Explanation:

NetFlow is a Layer 3 (network layer) protocol that collects and monitors IP traffic flows. It is typically configured on Layer 3 interfaces because it relies on IP information for traffic flow analysis, which is not available on Layer 2 interfaces. Layer 2 interfaces handle frames within

the local network, and they don't have IP-related details that NetFlow uses to generate traffic statistics.

Question 8

Question Type: MultipleChoice

In regard to the Advanced Routing Engine (ARE), what must be enabled first when configuring a logical router on a PAN-OS firewall?

Options:

- A- License
- B- Plugin
- C- Content update
- D- General setting

Answer:

A

Explanation:

To enable the Advanced Routing Engine (ARE) on a Palo Alto Networks firewall, the license for the ARE must be applied first. Without the proper license, the firewall cannot activate and use the advanced routing features provided by ARE, such as support for more complex routing protocols (e.g., BGP, OSPF, etc.).

Once the license is applied and validated, the routing engine can be configured, allowing the creation of logical routers and routing policies.

Question 9

Question Type: MultipleChoice

Which forwarding methods can be used on the Objects tab when configuring the Log Forwarding profile?

Options:

- A- Panorama, syslog, email
- B- Syslog, HTTP, NetFlow
- C- Panorama, ADEM, syslog
- D- SNMP, HTTP, RADIUS

Answer:

A

Explanation:

When configuring the Log Forwarding profile on a Palo Alto Networks firewall, the forwarding methods available include:

Panorama: For forwarding logs to a Panorama management system.

Syslog: For forwarding logs to a syslog server.

Email: For sending logs via email.

Question 10

Question Type: MultipleChoice

By default, which type of traffic is configured by service route configuration to use the management interface?

Options:

- A- Security zone
- B- IPSec tunnel
- C- Virtual system (VSYS)
- D- Autonomous Digital Experience Manager (ADEM)

Answer:

D

Explanation:

By default, the Autonomous Digital Experience Manager (ADEM) traffic is configured to use the management interface in a Palo Alto Networks firewall. The management interface is typically used for management-related traffic, such as monitoring and logging, and it is configured to handle ADEM-related traffic for the optimal performance of digital experience monitoring features.

This default configuration helps ensure that ADEM traffic does not interfere with regular traffic that may traverse other interfaces, such as traffic from security zones or IPSec tunnels.



To Get Premium Files for NGFW-Engineer
Visit

<https://www.p2pexams.com/products/ngfw-engineer>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/ngfw-engineer>

20%
DISCOUNT

P2P
exams