

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

<https://www.2passeasy.com/dumps/NGFW-Engineer/>



NEW QUESTION 1

An organization runs multiple Kubernetes clusters both on-premises and in public clouds (AWS, Azure, GCP). They want to deploy the Palo Alto Networks CN-Series NGFW to secure east-west traffic within each cluster, maintain consistent Security policies across all environments, and dynamically scale as containerized workloads spin up or down. They also plan to use a centralized Panorama instance for policy management and visibility. Which approach meets these requirements?

- A. Install standalone CN-Series instances in each cluster with local configuration only
- B. Export daily policy configuration snapshots to Panorama for recordkeeping, but do not unify policy enforcement.
- C. Configure the CN-Series only in public cloud clusters, and rely on Kubernetes Network Policies for on-premises cluster security
- D. Synchronize partial policy information into Panorama manually as needed.
- E. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in each cluster, ensuring local insertion into the service mesh or CN
- F. Manage all CN-Series firewalls centrally from Panorama, applying uniform Security policies across on-premises and cloud clusters.
- G. Deploy a single CN-Series firewall in the on-premises data center to process traffic for all clusters, connecting remote clusters via VPN or peerin
- H. Manage this single instance through Panorama.

Answer: C

Explanation:

This approach meets all the requirements for securing east-west traffic within each Kubernetes cluster, maintaining consistent security policies across on-premises and cloud environments, and allowing for dynamic scaling of the CN-Series NGFWs as containerized workloads spin up or down. By using Kubernetes-native deployment tools (such as Helm), the CN-Series NGFWs can be deployed and scaled dynamically within each cluster. Local insertion into the service mesh or CNI ensures that the NGFW can inspect traffic at the appropriate points within the cluster. Centralized management via Panorama ensures that security policies are uniform across both on-premises and cloud environments, providing visibility and control across all clusters.

NEW QUESTION 2

What is the purpose of assigning an Admin Role Profile to a user in a Palo Alto Networks NGFW?

- A. Allow access to all resources without restrictions.
- B. Enable multi-factor authentication (MFA) for administrator access.
- C. Define granular permissions for management tasks.
- D. Restrict access to sensitive report data.

Answer: C

Explanation:

Assigning an Admin Role Profile to a user in a Palo Alto Networks NGFW is used to define granular permissions for management tasks. This allows administrators to control what actions a user can perform on the firewall, such as configuration changes, monitoring, and logging. By assigning different admin roles, you can ensure that users have access only to the areas and tasks they need, enforcing the principle of least privilege.

NEW QUESTION 3

An NGFW engineer is configuring multiple Panorama-managed firewalls to start sending all logs to Strata Logging Service. The Strata Logging Service instance has been provisioned, the required device certificates have been installed, and Panorama and the firewalls have been successfully onboarded to Strata Logging Service.

Which configuration task must be performed to start sending the logs to Strata Logging Service and continue forwarding them to the Panorama log collectors as well?

- A. Modify all active Log Forwarding profiles to select the ??Cloud Logging?? option in each profile match list in the appropriate device groups.
- B. Enable the ??Panorama/Cloud Logging?? option in the Logging and Reporting Settings section under Device --> Setup --> Management in the appropriate templates.
- C. Select the ??Enable Duplicate Logging?? option in the Cloud Logging section under Device--> Setup --> Management in the appropriate templates.
- D. Select the ??Enable Cloud Logging?? option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.

Answer: D

Explanation:

To begin sending logs to Strata Logging Service while continuing to forward them to Panorama log collectors, the necessary configuration is to enable Cloud Logging. This option is configured in the Cloud Logging section under Device Setup Management in the appropriate templates. Once enabled, this ensures that logs are directed both to the Strata Logging Service (cloud) and to the Panorama log collectors.

NEW QUESTION 4

Which statement applies to the relationship between Panorama-pushed Security policy and local firewall Security policy?

- A. When a policy match is found in a local firewall policy, if any Panorama shared post-rule is configured, it will still be evaluated.
- B. Local firewall rules are evaluated after Panorama pre-rules and before Panorama post-rules.
- C. Panorama post-rules can be configured to be evaluated before local firewall policy for the purpose of troubleshooting.
- D. The order of policy evaluation can be configured differently in different device groups.

Answer: B

Explanation:

Local firewall rules are evaluated after Panorama pre-rules (those applied before the firewall's local policies) and before Panorama post-rules (those applied after the firewall's local policies). This ensures that the local firewall rules do not override the central Panorama policy and are only applied in the appropriate order within the policy evaluation sequence.

NEW QUESTION 5

Which PAN-OS method of mapping users to IP addresses is the most reliable?

- A. Port mapping
- B. GlobalProtect
- C. Syslog
- D. Server monitoring

Answer: D

Explanation:

Server monitoring is the most reliable method for mapping users to IP addresses in PAN- OS. This method allows the firewall to monitor specific servers, such as Microsoft Active Directory (AD) or LDAP servers, to dynamically retrieve and update user-to-IP mappings. It provides a more accurate and up-to-date mapping of users to their associated IP addresses, as it directly queries user databases in real time.

NEW QUESTION 6

Which configuration step is required when implementing a new self-signed root certificate authority (CA) certificate for SSL decryption on a Palo Alto Networks firewall?

- A. Import the new subordinate CA certificate into the trust stores of all client devices.
- B. Set the subordinate CA certificate as the default routing certificate for all network traffic.
- C. Configure the subordinate CA to issue certificates with indefinite validity periods.
- D. Disable all existing SSL decryption rules until the new certificate is fully propagated.

Answer: A

Explanation:

When implementing a new self-signed root certificate authority (CA) for SSL decryption on a Palo Alto Networks firewall, the subordinate CA certificate (which is generated by the firewall) must be imported into the trust stores of all client devices. This ensures that client devices trust the firewall as a valid certificate authority, enabling the firewall to decrypt and re-encrypt SSL traffic.

Importing the subordinate CA certificate into the client devices' trust stores is necessary for those devices to trust the new self-signed root CA and properly handle SSL decryption traffic.

NEW QUESTION 7

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

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

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.

NEW QUESTION 8

Which type of firewall resource can be assigned when configuring a new firewall virtual system (VSYS)?

- A. ICPU
- B. Sessions limit
- C. Memory
- D. Security profile limit

Answer: B

Explanation:

When configuring a new firewall virtual system (VSYS) on a Palo Alto Networks firewall, one of the resources that can be assigned is the sessions limit. This setting allows the administrator to control the number of active sessions that can be handled by the VSYS, ensuring that each virtual system has an appropriate allocation of resources based on its needs.

NEW QUESTION 9

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

- 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.

NEW QUESTION 10

For which two purposes is an IP address configured on a tunnel interface? (Choose two.)

- A. Use of dynamic routing protocols
- B. Tunnel monitoring
- C. Use of peer IP
- D. Redistribution of User-ID

Answer: AB

Explanation:

Use of dynamic routing protocols: An IP address is needed on the tunnel interface to participate in dynamic routing protocols (like OSPF, BGP, etc.) over the tunnel. This allows the firewall to advertise routes and receive updates over the tunnel.

Tunnel monitoring: The IP address on the tunnel interface can also be used for monitoring the tunnel's status. Tunnel monitoring (such as IPSec tunnel monitoring) requires an IP address on the tunnel interface to check the health and availability of the tunnel.

NEW QUESTION 10

Which two zone types are valid when configuring a new security zone? (Choose two.)

- A. Tunnel
- B. Intrazone
- C. Internal
- D. Virtual Wire

Answer: AD

Explanation:

When configuring a new security zone on a Palo Alto Networks firewall, the two valid zone types are:

Tunnel: A Tunnel zone is used for traffic that is associated with a VPN tunnel, such as IPSec tunnels. Traffic passing through a tunnel interface is classified into this zone.

Virtual Wire: A Virtual Wire zone is used when a firewall operates in transparent mode (also known as Layer 2 mode). In this configuration, the firewall can inspect traffic without modifying the IP address structure of the network.

NEW QUESTION 12

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?

- A. Create one CIE tenant, aggregate all identity data into a single view, and redistribute the full dataset to all firewall
- B. Rely on per-firewall Security policies to restrict access to out-of-scope user and group information.
- C. Establish separate CIE tenants for each business unit, integrating each tenant with the relevant identity source
- D. 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.
- E. Disable redistribution of identity data entirely
- F. Instead, configure each regional firewall to pull user and group details directly from its local identity providers (IdPs).
- G. 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.

NEW QUESTION 14

Which configuration in the LACP tab will enable pre-negotiation for an Aggregate Ethernet (AE) interface on a Palo Alto Networks high availability (HA) active/passive pair?

- A. Set Transmission Rate to `fast`.
- B. Set passive link state to `Auto`.
- C. Set `Enable in HA Passive State`.
- D. Set LACP mode to `Active`.

Answer: C

Explanation:

In a High Availability (HA) active/passive pair configuration, when setting up an Aggregate Ethernet (AE) interface, enabling the "Enable in HA Passive State" option allows the interface to participate in LACP (Link Aggregation Control Protocol) even when the system is in the passive state. This ensures that the pre-negotiation of the LACP link occurs, allowing the link aggregation to be ready as soon as the firewall becomes active.

NEW QUESTION 16

In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.

What function do certificate profiles serve in this context?

- A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.
- B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for

user or device authentication.

- C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.
- D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.

Answer: B

Explanation:

In the context of GlobalProtect with certificate-based authentication, certificate profiles are used to ensure proper validation of the certificates. They perform the following functions: Define trust anchors, which are the root and intermediate Certificate Authorities (CAs) that the firewall trusts to authenticate certificates. Specify revocation checks, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked.

Map certificate attributes, such as the Common Name (CN), which helps in authenticating users and devices based on their certificates.

NEW QUESTION 18

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.)

- 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: CD

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.

NEW QUESTION 21

An NGFW engineer is establishing bidirectional connectivity between the accounting virtual system (VSYS) and the marketing VSYS. The traffic needs to transition between zones without leaving the firewall (no external physical connections). The interfaces for each VSYS are assigned to separate virtual routers (VRs), and inter-VR static routes have been configured. An external zone has been created correctly for each VSYS. Security policies have been added to permit the desired traffic between each zone and its respective external zone. However, the desired traffic is still unable to successfully pass from one VSYS to the other in either direction.

Which additional configuration task is required to resolve this issue?

- A. Create a transit VSYS and route all inter-VSYS traffic through it.
- B. Add each VSYS to the list of visible virtual systems of the other VSYS.
- C. Enable the ??allow inter-VSYS traffic?? option in both external zone configurations.
- D. Create Security policies to allow the traffic between the two external zones.

Answer: B

Explanation:

In Palo Alto Networks firewalls, each virtual system (VSYS) is typically isolated from other VSYSs, meaning that traffic between different VSYSs cannot pass through the firewall by default. In this case, since the interfaces for each VSYS are assigned to separate virtual routers (VRs), and the desired traffic is still not passing between the two VSYSs, the firewall needs to be explicitly configured to allow traffic between them.

The required configuration is to add each VSYS to the list of visible virtual systems of the other VSYS. This allows inter-VSYS communication to be enabled, effectively permitting the traffic to pass between the zones of different VSYSs.

NEW QUESTION 24

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NGFW-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NGFW-Engineer Product From:

<https://www.2passeasy.com/dumps/NGFW-Engineer/>

Money Back Guarantee

NGFW-Engineer Practice Exam Features:

- * NGFW-Engineer Questions and Answers Updated Frequently
- * NGFW-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * NGFW-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NGFW-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year