

Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall 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 onl
- 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 securit
- D. Synchronize partial policy information into Panorama manually as needed.
- E. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in eachcluster, 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

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 4

Which interface types should be used to configure link monitoring for a high availability (HA) deployment on a Palo Alto Networks NGFW?

- A. HA, Virtual Wire, and Layer 2
- B. Tap, Virtual Wire, and Layer 3
- C. Virtual Wire, Layer 2, and Layer 3
- D. HA, Layer 2. and Layer 3

Answer: C

Explanation:

When configuring link monitoring for high availability (HA) on a Palo Alto Networks NGFW, the following interface types are supported:

Virtual Wire: Used when you have a transparent mode firewall deployment, where the firewall operates at Layer 2 to monitor traffic between two network segments.

Layer 2: Also used in transparent mode, where the firewall operates as a Layer 2 device and can be configured for link monitoring.

Layer 3: Used in routed mode, where the firewall is involved in routing traffic and can also be configured to monitor links.

NEW QUESTION 5

What must be configured before a firewall administrator can define policy rules based on users and groups?

- A. User Mapping profile
- B. Authentication profile

- C. Group mapping settings
- D. LDAP Server profile

Answer: C

Explanation:

Before a firewall administrator can define policy rules based on users and groups, the Group Mapping settings must be configured. These settings enable the firewall to map users to their respective Active Directory (AD) groups. This mapping allows the firewall to use user and group information to create policy rules based on group membership.

NEW QUESTION 6

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 7

An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logout stage and SAML-based multi-factor authentication (MFA) for user login.

How does the GlobalProtect agent process the authentication flow on Windows endpoints?

- A. The GlobalProtect agent uses the machine certificate to establish a pre-logout tunnel; upon user sign-in, it prompts for SAML-based MFA credentials, ensuring both device and user identities are validated before granting full access.
- B. The GlobalProtect agent uses the machine certificate during pre-logout for initial tunnel establishment, and then seamlessly reuses the same machine certificate for user-based authentication without requiring MFA.
- C. Once the machine certificate is validated at pre-logout, the Windows endpoint completes MFA on behalf of the user by passing existing Windows Credential Provider details to the GlobalProtect gateway without prompting the user.
- D. GlobalProtect requires the user to log in first for SAML-based MFA before establishing the pre-logout tunnel, rendering the pre-logout certificate authentication (CA) flow redundant.

Answer: A

Explanation:

In a hybrid authentication model with both certificate-based authentication for pre-logout and SAML-based multi-factor authentication (MFA) for user login, the GlobalProtect agent processes the flow as follows:

During the pre-logout stage, the agent uses the machine certificate to authenticate and establish the initial VPN tunnel.

Once the user logs in (after the machine is connected), the agent then triggers SAML-based MFA to ensure the user is authenticated with multi-factor authentication, validating both the device and the user identity before granting full access.

This method ensures that both the device and user are properly authenticated and validated in the hybrid authentication model.

NEW QUESTION 8

When deploying Palo Alto Networks NGFWs in a cloud service provider (CSP) environment, which method ensures high availability (HA) across multiple availability zones?

- A. Deploying Ansible scripts for zone-specific scaling
- B. Implementing Terraform templates for redundancy within one availability zone
- C. Using load balancer and health probes
- D. Configuring active/active HA

Answer: C

Explanation:

To ensure high availability (HA) across multiple availability zones (AZs) in a cloud service provider (CSP) environment, using a load balancer with health probes is a recommended method. This setup ensures that traffic can be directed to the healthy NGFW instances across multiple availability zones. If one NGFW instance or availability zone goes down, the load balancer can redirect traffic to the available instance(s) in other zones, providing redundancy and maintaining service availability.

NEW QUESTION 9

A large enterprise wants to implement certificate-based authentication for both users and devices, using an on-premises Microsoft Active Directory Certificate Services (AD CS) hierarchy as the primary certificate authority (CA). The enterprise also requires Online Certificate Status Protocol (OCSP) checks to ensure efficient revocation status updates and reduce the overhead on its NGFWs. The environment includes multiple Active Directory forests, Panorama management for several geographically dispersed firewalls, GlobalProtect portals and gateways needing distinct certificate profiles for users and devices, and strict Security policies demanding frequent revocation checks with minimal latency.

Which approach best addresses these requirements while maintaining consistent policy enforcement?

- A. Deploy self-signed certificates at each site to simplify local certificate validation and reduce dependencies on a centralized C
- B. Turn off certificate revocation checks for lower overhead, rely on IP-based rules for GlobalProtect authentication, and use a single certificate profile for both users and devices.
- C. Distribute the root and intermediate CA certificates via Panorama as shared objects to ensure all firewalls have a consistent trust chain
- D. Configure OCSP responder profiles on each firewall to offload revocation checks to an internal OCSP server while keeping CRL checks as a fallback

- E. Maintain separate certificate profiles for user and device authentication and use an automated enrollment method – such as Group Policy or SCEP – to deploy certificates to endpoints.
- F. Configure each firewall independently to trust the root and intermediate CA certificate
- G. Rely only on manual CRL checks for certificate revocation, and import both user and device certificates directly into each firewall's local certificate store for authentication.
- H. Obtain wildcard certificates from a public CA for both user and device authentication, and configure firewalls to perform CRL polling at the default update interval.
- I. Manually install user certificates on endpoints and synchronize firewall certificate stores through frequent manual SSH updates to maintain consistency.

Answer: B

Explanation:

This approach best addresses the enterprise's requirements for certificate-based authentication, OCSP checks, and consistent policy enforcement:

Distributing the root and intermediate CA certificates via Panorama ensures that all firewalls in the enterprise are consistent in their trust chain and can validate certificates properly.

Configuring OCSP responder profiles on each firewall offloads the revocation checks to an internal OCSP server, which reduces the overhead on the firewalls and ensures fast, real-time certificate status checks.

Using CRL checks as a fallback ensures reliability in case the OCSP responder is unavailable.

Separate certificate profiles for users and devices ensure that the firewall can enforce different security policies based on the type of certificate (user vs. device).

Automated certificate enrollment methods such as Group Policy or SCEP streamline certificate distribution to endpoints, ensuring efficient management of certificates across geographically dispersed firewalls.

NEW QUESTION 10

An NGFW engineer is configuring multiple Layer 2 interfaces on a Palo Alto Networks firewall, and all interfaces must be assigned to the same VLAN. During initial testing, it is reported that clients located behind the various interfaces cannot communicate with each other.

Which action taken by the engineer will resolve this issue?

- A. Configure each interface to belong to the same Layer 2 zone and enable IP routing between them.
- B. Assign each interface to the appropriate Layer 2 zone and configure a policy that allows traffic within the VLAN.
- C. Assign each interface to the appropriate Layer 2 zone and configure Security policies for interfaces not assigned to the same zone.
- D. Enable IP routing between the interfaces and configure a Security policy to allow traffic between interfaces within the VLAN.

Answer: B

Explanation:

In a Layer 2 configuration, interfaces are typically grouped into the same Layer 2 zone. When the interfaces are assigned to the same VLAN, the firewall will treat them as part of the same broadcast domain.

In a Layer 2 setup, interfaces must be in the same Layer 2 zone to allow the traffic within the same VLAN to pass. Additionally, a security policy must be configured to allow traffic within this VLAN or zone. This will resolve the issue by ensuring that traffic is permitted between clients behind different interfaces assigned to the same VLAN.

NEW QUESTION 10

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 13

In an active/active high availability (HA) configuration with two PA-Series firewalls, how do the firewalls use the HA3 interface?

- A. To forward packets to the HA peer during session setup and asymmetric traffic flow
- B. To exchange hellos, heartbeats, HA state information, and management plane synchronization for routing and User-ID information
- C. To synchronize sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in an HA pair
- D. To perform session cache synchronization among all HA peers having the same cluster ID

Answer: D

Explanation:

In an active/active HA configuration with two PA-Series firewalls, the HA3 interface is used primarily for the exchange of HA state information between the firewalls. This includes: Hellos and heartbeats to monitor the status of the HA peer.

Synchronization of management plane data, which includes critical routing and User-ID information.

NEW QUESTION 16

During an upgrade to the routing infrastructure in a customer environment, the network administrator wants to implement Advanced Routing Engine (ARE) on a Palo Alto Networks firewall.

Which firewall models support this configuration?

- A. PA-5280, PA-7080, PA-3250, VM-Series
- B. PA-455, VM-Series, PA-1410, PA-5450
- C. PA-3260, PA-5410, PA-850, PA-460
- D. PA-7050, PA-1420, VM-Series, CN-Series

Answer: C

Explanation:

The Advanced Routing Engine (ARE) is supported on Palo Alto Networks firewalls that utilize the PAN-OS 11.0+ software and have the required hardware architecture. The supported models include PA-3200 Series, PA-5400 Series, PA-800 Series, and PA-400 Series. These models provide enhanced routing capabilities, including BGP, OSPF, and more complex routing policies.

PA-3260 and PA-5410 are part of the PA-3200 and PA-5400 Series, which are known to support ARE.

PA-850 and PA-460 are within the PA-800 and PA-400 Series, which also support ARE

NEW QUESTION 19

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 21

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 orreissue 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 25

Which two statements describe an external zone in the context of virtual systems (VSYS) on a Palo Alto Networks firewall? (Choose two.)

- A. It is associated with an interface within a VSYS of a firewall.
- B. It is a security object associated with a specific virtual router of a VSYS.
- C. It is not associated with an interface; it is associated with a VSYS itself.
- D. It is a security object associated with a specific VSYS.

Answer: AD

Explanation:

In the context of virtual systems (VSYS) on a Palo Alto Networks firewall, the external zone is typically associated with specific interfaces within a VSYS. Zones are fundamental security objects used to define traffic flow between interfaces, and the external zone would be used for interfaces that connect to external networks.

An external zone is associated with an interface within a VSYS of the firewall. This ensures that traffic from specific interfaces can be classified as belonging to the external zone, allowing the firewall to apply appropriate security policies.

The external zone is indeed a security object that is specific to a given VSYS, as each VSYS can have its own set of zones that are isolated from others.

NEW QUESTION 30

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 35

Which set of options is available for detailed logs when building a custom report on a Palo Alto Networks NGFW?

- A. Traffic, User-ID, URL
- B. Traffic, threat, data filtering, User-ID
- C. GlobalProtect, traffic, application statistics
- D. Threat, GlobalProtect, application statistics, WildFire submissions

Answer: B

Explanation:

When building a custom report on a Palo Alto Networks NGFW, you can select detailed logs that provide specific insights into various aspects of firewall activity. The available options for detailed logs typically include:

Traffic logs: These provide information on the network traffic passing through the firewall. Threat logs: These logs capture data related to identified security threats, such as malware or intrusion attempts.

Data filtering logs: These logs capture events related to data filtering policies, such as preventing the transfer of sensitive data.

User-ID logs: These logs associate user identities with the traffic and activities observed on the firewall, enabling user-based policy enforcement.

NEW QUESTION 39

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The NGFW-Engineer Practice Test Here](#)