

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

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



NEW QUESTION 1

An enterprise uses GlobalProtect with both user- and machine-based certificate authentication and requires pre-logon, OCSP checks, and minimal user disruption. They manage multiple firewalls via Panorama and deploy domain-issued machine certificates via Group Policy. Which approach ensures continuous, secure connectivity and consistent policy enforcement?

- A. Use a wildcard certificate from a public CA, disable all revocation checks to reduce latency, and manage certificate renewals manually on each firewall.
- B. Distribute root and intermediate CAs via Panorama template, use distinct certificate profiles for user versus machine certs, reference an internal OCSP responder, and automate certificate deployment with Group Policy.
- C. Configure a single certificate profile for both user and machine certificate
- D. Rely solely on CRLs for revocation to minimize complexity.
- E. Deploy self-signed certificates on each firewall, allow IP-based authentication to override certificate checks, and use default GlobalProtect settings for user / machine identification.

Answer: B

Explanation:

To ensure continuous, secure connectivity and consistent policy enforcement with GlobalProtect in an enterprise environment that uses user- and machine-based certificate authentication, the approach should:

Distribute root and intermediate CAs via Panorama templates: This ensures that all firewalls managed by Panorama share the same trusted certificate authorities for consistency and security.

Use distinct certificate profiles for user vs. machine certificates: This enables separate handling of user and machine authentication, ensuring that both types of certificates are managed and validated appropriately.

Reference an internal OCSP responder: By integrating OCSP checks, the firewall can validate certificate revocation in real-time, meeting the security requirement while minimizing the overhead and latency associated with traditional CRLs (Certificate Revocation Lists).

Automate certificate deployment with Group Policy: This ensures that machine certificates are deployed in a consistent and scalable manner across the enterprise, reducing manual intervention and minimizing user disruption.

This approach supports the requirements for pre-logon, OCSP checks, and minimal user disruption, while maintaining a secure, automated, and consistent authentication process across all firewalls managed via Panorama.

NEW QUESTION 2

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

- 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.

NEW QUESTION 3

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

- 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.

NEW QUESTION 4

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 5

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 6

An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The application will be able to make any approved changes directly to devices via API.

What is a requirement for the application to create SD-WAN interfaces?

- A. REST API's `sdwanInterfaceProfiles` parameter on a Panorama device
- B. REST API's `sdwanInterfaces` parameter on a firewall device
- C. XML API's `sdwanprofiles/interfaces` parameter on a Panorama device
- D. XML API's `InterfaceProfiles/sdwan` parameter on a firewall device

Answer: B

Explanation:

To create SD-WAN interfaces through an API, the correct approach is to use the REST API's "sdwanInterfaces" parameter on a firewall device. This parameter allows you to configure SD-WAN interfaces directly on the firewall devices via API, ensuring that the required interfaces are set up and managed for SD-WAN functionality.

NEW QUESTION 7

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

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

- A. The GlobalProtect agent uses the machine certificate to establish a pre-logon 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-logon 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-logon, 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-logon tunnel, rendering the pre-logon certificate authentication (CA) flow redundant.

Answer: A

Explanation:

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

During the pre-logon 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

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 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

Palo Alto Networks NGFWs use SSL/TLS profiles to secure which two types of connections? (Choose two.)

- A. NAT tables
- B. User Authentication
- C. GlobalProtect Gateways
- D. GlobalProtect Portal

Answer: CD

Explanation:

Palo Alto Networks Next-Generation Firewalls (NGFWs) use SSL/TLS profiles to secure connections for services such as GlobalProtect Gateways and GlobalProtect Portals. These profiles are used to manage the SSL/TLS encryption and decryption for secure communication between the firewall and clients (such as VPN clients for GlobalProtect). This helps ensure the confidentiality and integrity of the data during transmission.

NEW QUESTION 10

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

- 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 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).

NEW QUESTION 14

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 16

Without performing a context switch, which set of operations can be performed that will affect the operation of a connected firewall on the Panorama GUI?

- A. Restarting the local firewall, running a packet capture, accessing the firewall CLI
- B. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostname
- C. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network Profile
- D. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reports

Answer: B

Explanation:

In Panorama, without performing a context switch, the administrator can perform local configuration tasks directly on the connected firewall. The following operations can be done:

Modification of local security rules: Security rules can be modified directly on the connected firewall from the Panorama GUI.

Modification of a Layer 3 interface: Changes to the Layer 3 interfaces on the connected firewall can be done from Panorama, without needing to switch to the firewall's local interface.

Modification of the firewall device hostname: The firewall's hostname can be changed via Panorama.

NEW QUESTION 21

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 26

In a hybrid cloud deployment, what is the primary function of Ansible in managing Palo Alto Networks NGFWs?

- A. It provides a web interface for managing NGFW hardware clusters.
- B. It enables centralized log collection and correlation for NGFWs.
- C. It facilitates dynamic updates to NGFW threat databases.
- D. It automates NGFW policy updates and configurations through playbooks.

Answer: D

Explanation:

In a hybrid cloud deployment, Ansible is primarily used for automating configurations and policy updates on Palo Alto Networks Next-Generation Firewalls (NGFWs). Through the use of playbooks, Ansible can automate the process of deploying security policies, updating configurations, and managing the firewall's state, which enhances efficiency and consistency across multiple NGFWs in a large or hybrid cloud environment.

NEW QUESTION 31

To maintain security efficacy of its public cloud resources by using native tools, a company purchases Cloud NGFW credits to replicate the Panorama, PA-Series, and VM-Series devices used in physical data centers. Resources exist on AWS and Azure:

The AWS deployment is architected with AWS Transit Gateway, to which all resources connect

The Azure deployment is architected with each application independently routing traffic The engineer deploying Cloud NGFW in these two cloud environments must account for the following:

Minimize changes to the two cloud environments

Scale to the demands of the applications while using the least amount of compute resources

Allow the company to unify the Security policies across all protected areas Which two implementations will meet these requirements? (Choose two.)

- A. Deploy a VM-Series firewall in AWS in each VPC, create an IPSec tunnel between AWS and Azure, and manage the policy with Panorama.
- B. Deploy Cloud NGFW for Azure in vNET/s, update the vNET/s routing to path traffic through the deployed NGFWs, and manage the policy with Panorama.
- C. Deploy Cloud NGFW for Azure in vWAN, create a vWAN to route all appropriate traffic to the Cloud NGFW attached to the vWAN, and manage the policy with local rules.
- D. Deploy Cloud NGFW for AWS in a centralized Security VPC, update the Transit Gateway to route all appropriate traffic through the Security VPC, and manage the policy with Panorama.

Answer: BD

Explanation:

To meet the company's requirements - minimizing changes to the cloud environments, optimizing compute resources, and unifying security policies - the best approach is to deploy Cloud NGFW solutions natively for AWS and Azure while managing policies centrally with Panorama.

In Azure, using Cloud NGFW for Azure deployed within vNETs allows traffic to be routed through security appliances efficiently without requiring a complete re-architecture. This approach aligns with Azure's existing routing mechanism while maintaining security.

In AWS, deploying Cloud NGFW for AWS in a centralized Security VPC and integrating it with AWS Transit Gateway enables traffic inspection for all connected

VPNs without modifying individual workloads. This method ensures efficient scaling and minimal infrastructure changes while maintaining security consistency.

NEW QUESTION 35

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

- 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.

NEW QUESTION 38

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 40

An administrator plans to upgrade a pair of active/passive firewalls to a new PAN-OS release. The environment is highly sensitive, and downtime must be minimized.

What is the recommended upgrade process for minimal disruption in this high availability (HA) scenario?

- A. Suspend the active firewall to trigger a failover to the passive firewall
- B. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operation
- C. Then fail traffic back and upgrade the remaining firewall.
- D. Shut down the currently active firewall and upgrade it offline, allowing the passive firewall to handle all traffic
- E. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluster
- F. Finally, upgrade the passive firewall while the newly upgraded unit remains active.
- G. Isolate both firewalls from the production environment and upgrade them in a separate, offline setup
- H. Reconnect them only after validating the new software version, resuming HA functionality once both units are fully upgraded and tested.
- I. Push the new PAN-OS version simultaneously to both firewalls, having them upgrade and reboot in parallel
- J. Rely on automated HA reconvergence to restore normal operations without manually failing over traffic.

Answer: A

Explanation:

In an active/passive HA setup, the recommended process for upgrading involves minimizing downtime and ensuring traffic continuity by using the failover process:

Suspend the active firewall: This triggers a failover to the passive unit, making it the active unit.

Upgrade the former passive (now active) unit: With traffic now running on the previously passive unit, upgrade the suspended unit while the active unit continues handling traffic. Confirm proper operation: Once the upgrade is complete, verify that the upgraded unit is functioning properly.

Fail traffic back: Once the upgraded firewall is confirmed to be working, fail the traffic back to the original active unit and upgrade the remaining firewall.

NEW QUESTION 44

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 46

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 50

.....

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