Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

NEW QUESTION 1
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 2
Which statement describes the role of Terraform in deploying Palo Alto Networks NGFWs?

A. It acts as a logging service for NGFW performance metrics.
B. It orchestrates real-time traffic inspection for network segments.
C. It provides Infrastructure-as-Code (IaC) to automate NGFW deployment.
D. It manages threat intelligence data synchronization with NGFWs.

Answer: C

Explanation:
Terraform is an Infrastructure-as-Code (IaC) tool that automates the provisioning and management of infrastructure resources, including Palo Alto Networks Next-Generation Firewalls (NGFWs). By using Terraform configuration files, administrators can define and deploy NGFW instances across cloud environments (such as AWS, Azure, and GCP) efficiently and consistently.
Terraform enables:
Automated firewall deployment in cloud environments.
Configuration of security policies and networking settings in a declarative manner. Scalability and repeatability, reducing manual intervention in firewall provisioning.

NEW QUESTION 3
Which zone type allows traffic between zones in different virtual systems (VSYS), without the traffic leaving the firewall?

A. Isolated
B. Transient
C. External
D. Internal

Answer: B

Explanation:
The Transient zone type is used to allow traffic between zones in different virtual systems (VSYS) on a Palo Alto Networks firewall without the traffic leaving the firewall. It provides a way for virtual systems to communicate with each other by acting as a temporary or intermediary zone. Traffic can pass through the firewall between the virtual systems without requiring physical interfaces or leaving the device.

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 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 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
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 9
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 10
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 10
What are the phases of the Palo Alto Networks AI Runtime Security: Network Intercept solution?

A. Scanning, Isolation, Whitelisting, Logging
B. Discovery, Deployment, Detection, Prevention
C. Policy Generation, Discovery, Enforcement, Logging
D. Profiling, Policy Generation, Enforcement, Reporting

Answer: B

Explanation:
The phases of the Palo Alto Networks AI Runtime Security: Network Intercept solution are designed to help identify and protect against potential threats in real time by using AI to detect and prevent malicious activities within the network.
Discovery: Identifying applications, services, and behaviors within the network to understand baseline activity.
Deployment: Implementing the solution into the network and integrating with existing security measures.
Detection: Monitoring traffic and activities to identify abnormal or malicious behavior. Prevention: Taking action to stop threats once detected, such as blocking malicious traffic or stopping exploit attempts.

NEW QUESTION 11
How does a Palo Alto Networks NGFW respond when the preemptive hold time is set to 0 minutes during configuration of route monitoring?

A. It does not accept the configuration.
B. It accepts the configuration but throws a warning message.
C. It removes the static route because 0 is a NULL value
D. It reinstalls the route into the routing information base (RIB) as soon as the path comes up.

Answer: D

Explanation:
When the preemptive hold time is set to 0 minutes in route monitoring, the firewall is configured to immediately reinstall the route into the Routing Information Base (RIB) as soon as the monitored path comes up. This essentially means that the firewall will not wait for any predefined hold time before reestablishing the route once the monitoring condition is met, ensuring a faster recovery of the route.

NEW QUESTION 16
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 VPCs without modifying individual workloads. This method ensures efficient scaling and minimal infrastructure changes while maintaining security consistency.

NEW QUESTION 19
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 firewal
B. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operatio
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 traffi
E. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluste
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 setu
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 paralle
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 21
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 24
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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