Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 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 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 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
A PA-Series firewall with all licensable features is being installed. The customer??s Security policy requires that users do not directly access websites. Instead, a security device must create the connection, and there must be authentication back to the Active Directory servers for all sessions.
Which action meets the requirements in this scenario?

A. Deploy the transparent proxy with Web Cache Communications Protocol (WCCP).
B. Deploy the Next-Generation Firewalls as normal and install the User-ID agent.
C. Deploy the Advanced URL Filtering license and captive portal.
D. Deploy the explicit proxy with Kerberos authentication scheme.

Answer: D

Explanation:

In this scenario, the customer requires that users do not directly access websites and that a security device (the firewall) manages the connection, while also ensuring that there is authentication back to the Active Directory (AD) servers for all sessions. The explicit proxy with Kerberos authentication is the best solution because:
The explicit proxy allows the firewall to intercept user web traffic and manage the connections on behalf of users.
Kerberos authentication ensures that the user??s identity is validated against the Active Directory servers before the session is allowed, fulfilling the authentication requirement.

NEW QUESTION 6
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 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
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 9
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 10
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 10
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 15
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 20
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 25
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 27
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 28
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 32
.....

Relate Links

100% Pass Your NGFW-Engineer Exam with Exambible Prep Materials

https://www.exambible.com/NGFW-Engineer-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/