[2026-January-NewBraindump2go NGFW-Engineer Dumps PDF Free[Q1-Q32

2026/January Latest Braindump2go NGFW-Engineer Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go NGFW-Engineer Real Exam Questions!QUESTION 1In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.What function do certificate profiles serve in this context?A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for user or device authentication.C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.Answer: BExplanation: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Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked.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.QUESTION 2How 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 valueD. It reinstalls the route into the routing information base (RIB) as soon as the path comes up.Answer: DExplanation: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.QUESTION 3After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish. Which of the following actions will resolve this issue?A. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.B. Configure the Proxy IDs to match the Cisco ASA configuration.C. Check that IPSec is enabled in the management profile on the external interface.D. Validate the tunnel interface VLAN against the peer's configuration.Answer: BExplanation:The Proxy IDs (or Traffic Selectors) define the local and remote subnets that are allowed to communicate over the IPSec tunnel. If the Proxy IDs on the Palo Alto Networks firewall do not match the configuration on the Cisco ASA, the tunnel will fail to establish because the firewalls won't agree on which traffic to encrypt. Ensuring that the Proxy IDs match between the Palo Alto Networks firewall and the Cisco ASA will resolve the issue.QUESTION 4Which 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: DExplanation:On a Palo Alto Networks firewall, LACP pre-negotiation means the interface actively sends LACP packets to negotiate the aggregate link instead of waiting for the peer.LACP mode = Active ? The device initiates LACP negotiations by sending LACP PDUs.LACP mode = Passive ? The device waits for the peer to initiate, so no pre-negotiation occurs.QUESTION 5When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?A. Service graphB. Ansible automation modulesC. Panorama role-based access controlD. CN-Series firewallsAnswer: DExplanation: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.QUESTION 6 When configuring a Zone Protection profile, in which section (protection type) would an NGFW engineer configure options to protect against activities such as spoofed IP addresses and split handshake session establishment attempts?A. Flood ProtectionB. Protocol ProtectionC. Packet-Based Attack ProtectionD. Reconnaissance ProtectionAnswer: CExplanation:Packet-Based Attack Protection examines IP, TCP, ICMP, IPv6, and ICMPv6 packet headers to drop packets with undesirable characteristics like IP spoofing or malformed TCP options that enable split handshakes.QUESTION 7For which two purposes is an IP address configured on a tunnel interface? (Choose two.)A. Use of dynamic routing protocolsB. Tunnel monitoringC. Use of peer IPD. Redistribution of User-IDAnswer: ABExplanation:Use of dynamic routing protocols: An IP address is needed on the tunnel interface to participate in dynamic routing protocols (like OSPF, BGP, etc.) over the tunnel. This allows the firewall to advertise routes and

receive updates over the tunnel.Tunnel monitoring: The IP address on the tunnel interface can also be used for monitoring the tunnel's status. Tunnel monitoring (such as IPSec tunnel monitoring) requires an IP address on the tunnel interface to check the health and availability of the tunnel.QUESTION 8Which PAN-OS method of mapping users to IP addresses is the most reliable?A. Port mappingB. GlobalProtectC. SyslogD. Server monitoringAnswer: BExplanation:GlobalProtect provides accurate, timely mappings by requiring user authentication on network changes, device posture shifts, or logon events, using both internal and external gateways for comprehensive coverage across remote and on-premises users without relying on external agents or syslog delays.QUESTION 9In 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 flowB. To exchange hellos, heartbeats, HA state information, and management plane synchronization for routing and User-ID informationC. To synchronize sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in an HA pairD. To perform session cache synchronization among all HA peers having the same cluster IDAnswer: AExplanation:The HA3 interface, a Layer 2 link using MAC-in-MAC encapsulation, enables packet forwarding between active/active firewalls to handle asymmetric routing and ensure proper session setup when traffic arrives at the non-owner peer.QUESTION 10A 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: DExplanation: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.QUESTION 11What must be configured before a firewall administrator can define policy rules based on users and groups?A. User Mapping profileB. Authentication profileC. Group mapping settingsD. LDAP Server profileAnswer: CExplanation: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.QUESTION 12Which 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: BExplanation: 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.QUESTION 13Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?A. DDNSB. Link DuplexC. NetFlowD. LLDPAnswer: CExplanation:NetFlow is a Layer 3 (network layer) protocol that collects and monitors IP traffic flows. It is typically configured on Layer 3 interfaces because it relies on IP information for traffic flow analysis, which is not available on Layer 2 interfaces. Layer 2 interfaces handle frames within the local network, and they don't have IP-related details that NetFlow uses to generate traffic statistics.QUESTION 14What 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. lt 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: DExplanation: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).QUESTION 15According to dynamic updates best practices, what is the recommended threshold value for content updates in a mission- critical network?A. 8 hoursB. 16 hoursC. 32 hoursD. 48 hoursAnswer: 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.QUESTION 16An organization runs multiple Kubernetes clusters both on-premises and in public clouds (AWS, Azure, GCP). They want to deploy the Palo Alto Networks CN-Series NGFW to secure east-west traffic within each cluster, maintain consistent Security policies across all environments, and dynamically scale as containerized workloads spin up or down. They also plan to use a centralized Panorama instance for policy management and visibility.Which approach meets these requirements?A. Install standalone CN-Series instances in each cluster with local configuration only. Export daily policy configuration snapshots to Panorama for recordkeeping, but do not unify policy enforcement.B. Configure the CN-Series only in public cloud clusters, and rely on Kubernetes Network Policies for on-premises cluster security. Synchronize partial policy information into Panorama manually as needed.C. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in each cluster, ensuring local insertion into the service mesh or CNI. Manage all CN-Series firewalls centrally from Panorama, applying uniform Security policies across on-premises and cloud clusters.D. Deploy a single CN-Series firewall in the on-premises data center to process traffic for all clusters, connecting remote clusters via VPN or peering. Manage this single instance through Panorama.Answer: CExplanation: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.QUESTION 17When 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 scalingB. Implementing Terraform templates for redundancy within one availability zoneC. Using load balancer and health probesD. Configuring active/active HAAnswer: 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.QUESTION 18An 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 deviceB. REST API's "sdwanInterfaces" parameter on a firewall deviceC. XML API's "sdwanprofiles/interfaces" parameter on a Panorama deviceD. XML API's "InterfaceProfiles/sdwan" parameter on a firewall deviceAnswer: AExplanation:SD-WAN interfaces on Palo Alto firewalls are centrally managed through Panorama using the REST API endpoint for "sdwanInterfaceprofiles" in templates, which defines link characteristics before creating the virtual SD-WAN interfaces that group physical Ethernet links.QUESTION 19Which 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: CDExplanation: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.QUESTION 20An 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: CExplanation:External zones in Palo Alto firewalls require explicitly enabling "Allow traffic from other VSYS" (or similar inter-VSYS traffic allowance) in their zone configurations to permit bidirectional flow between VSYS without physical external routing, even when VSYS visibility, policies, and inter-VR routes are already configured.Why VSYS Visibility Alone FailsWhile adding VSYS to each other's visible list enables awareness of external zones across VSYS boundaries, traffic still drops unless the external zones themselves permit inter-VSYS traversal, as zones enforce isolation by default beyond mere visibility.QUESTION 21Without 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 CLIB. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostnameC. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network ProfileD. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reportsAnswer: CExplanation:From the Panorama GUI context, pre-rules (pre-security rules), virtual routers, and IKE Gateway Network Profiles are managed centrally through Device Groups and Templates, so modifications apply directly to firewalls after commit/push without needing to switch to the firewall's local context.QUESTION 22Which set of options is available for detailed logs when building a custom report on a Palo Alto Networks NGFW?A. Traffic, User-ID, URLB. Traffic, threat, data filtering, User-IDC. GlobalProtect, traffic, application statisticsD. Threat, GlobalProtect, application statistics, WildFire submissionsAnswer: BExplanation: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.QUESTION 23An 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. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operation. Then fail traffic back and upgrade the remaining firewall.B. Shut down the currently active firewall and upgrade it offline, allowing the passive firewall to handle all traffic. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluster. Finally, upgrade the passive firewall while the newly upgraded unit remains active.C. Isolate both firewalls from the production environment and upgrade them in a separate, offline setup. Reconnect them only after validating the new software version, resuming HA functionality once both units are fully upgraded and tested.D. Push the new PAN-OS version simultaneously to both firewalls, having them upgrade and reboot in parallel. Rely on automated HA reconvergence to restore normal operations without manually failing over traffic.Answer: AExplanation: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.QUESTION 24Which 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: ADExplanation: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.QUESTION 25Which zone type allows traffic between zones in different virtual systems (VSYS), without the traffic leaving the firewall?A. IsolatedB. TransientC. ExternalD. InternalAnswer: C Explanation:External zones enable inter-VSYS communication internally on the firewall by associating with a specific VSYS and allowing traffic to traverse to visible external zones of other VSYS, requiring VSYS visibility configuration and security policies from internal zones to/from the external zone.QUESTION 26A 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 firewalls. Rely on per-firewall Security policies to restrict access to out-of-scope user and group information.B. Establish separate CIE tenants for each business unit, integrating each tenant with the relevant identity sources. 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.C. Disable redistribution of identity data entirely. Instead, configure each regional firewall to pull user and group details directly from its local identity providers (IdPs).D. 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: BExplanation: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.QUESTION 27An engineer is implementing a new rollout of SAML for administrator authentication across a company's Palo Alto Networks NGFWs. User authentication on company firewalls is currently performed with RADIUS, which will remain available for six months, until it is decommissioned. The company wants both authentication types to be running in parallel during the transition to SAML.Which two actions meet the criteria? (Choose two.)A. Create a testing and rollback plan for the transition from Radius to SAML, as the two authentication profiles cannot be run in tandem.B. Create an authentication sequence that includes both the "RADIUS" Server Profile and "SAML Identity Provider" Server Profile to run the two services in tandem.C. Create and apply an authentication profile with the "SAML Identity Provider" Server Profile.D. Create and add the "SAML Identity Provider" Server Profile to the authentication profile for the "RADIUS" Server Profile.Answer: BCExplanation:B. Create an authentication sequence that orders the RADIUS profile first followed by the SAML profile, allowing the firewall to attempt RADIUS authentication and fall back to SAML if needed, supporting tandem operation for administrator logins.C. Create and apply an authentication profile using the SAML Identity Provider Server Profile, which can then be sequenced alongside the existing RADIUS profile without disrupting current authentication.QUESTION 28An 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 certificates. Rely solely on CRLs for revocation to minimize complexity.D. 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: BExplanation: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.QUESTION 29Which statement applies to Log Collector Groups?A. Log redundancy is available only if each Log Collector has the same amount of total disk storage.B. Enabling redundancy increases the log processing traffic in a Collector Group by 50%.C. In any single Collector Group, all the Log Collectors must run on the same Panorama model.D. The maximum number of Log Collectors in a Log Collector Group is 18 plus two hot spares.Answer: DExplanation:The maximum number of Log Collectors that can be added to a Log Collector Group is 18 plus 2 hot spares, ensuring redundancy and availability in case of failure. This allows for a total of up to 20 Log Collectors in a group, providing sufficient scalability and reliability for log collection.QUESTION 30Which 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 2B. Tap, Virtual Wire, and Layer 3C. Virtual Wire, Layer 2, and Layer 3D. HA, Layer 2. and Layer 3Answer: 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.QUESTION 31Which CLI command is used to configure the management interface as a DHCP client?A. set network dhcp interface managementB. set network dhcp type management-interfaceC. set deviceconfig system type dhcp-clientD. set deviceconfig management type dhcp-clientAnswer: DExplanation:To configure the management interface as a DHCP client on a Palo Alto Networks NGFW, the correct CLI command is set deviceconfig management type dhcp-client. This command configures the management interface to obtain an IP address dynamically using DHCP.QUESTION 32 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: AExplanation: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.Resources From:1.2026 Latest Braindump2go NGFW-Engineer Exam Dumps (PDF & VCE) Free Share:**https://www.braindump2go.com/ngfw-engineer.html**
2.2026 Latest Braindump2go NGFW-Engineer PDF and NGFW-Engineer VCE Dumps Free Share:
https://drive.google.com/drive/folders/18HMHamEShZ7h2LJfaE_2IT-WyPet_FmD?usp=sharing3.2026 Free Braindump2go NGFW-Engineer Exam Questions Download:
https://www.braindump2go.com/free-online-pdf/NGFW-Engineer-VCE-Dumps(1-32).pdf Free Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!