PaloAltoNetworks.NGFW-Engineer.v2026-05-13.q62

Exam Code:	NGFW-Engineer
Exam Name:	Palo Alto Networks Next-Generation Firewall Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	62
Version:	v2026-05-13
# of views:	138
# of Questions views:	620
https://www.freepdfdumps.com/PaloAltoNetworks.NGFW-Engineer.v2026-05-13.q62.html	

NEW QUESTION: 1
When deploying Palo Alto Networks NGFWs in a cloud service provider (CSP) environment, which method ensures high availability (HA) across multiple availability zones?
A. Deploying Ansible scripts for zone-specific scaling
B. Implementing Terraform templates for redundancy within one availability zone
C. Using load balancer and health probes
D. Configuring active/active HA
Answer: C (LEAVE A REPLY)
To ensure high availability (HA) across multiple availability zones (AZs) in a cloud service provider (CSP) environment, using a load balancer with health probes is a recommended method. This setup ensures that traffic can be directed to the healthy NGFW instances across multiple availability zones. If one NGFW instance or availability zone goes down, the load balancer can redirect traffic to the available instance(s) in other zones, providing redundancy and maintaining service availability.

NEW QUESTION: 2
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 (LEAVE A REPLY)
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: 3
In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.
What function do certificate profiles serve in this context?
A. They store private keys for users and devices, effectively allowing the firewall to issue 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: B (LEAVE A REPLY)
In the context of GlobalProtect with certificate-based authentication, certificate profiles are used to ensure proper validation of the certificates. They perform the following functions:
Define trust anchors, which are the root and intermediate Certificate Authorities (CAs) that the firewall trusts to authenticate certificates.
Specify revocation checks, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked.
Map certificate attributes, such as the Common Name (CN), which helps in authenticating users and devices based on their certificates.

NEW QUESTION: 4
A security engineer creates a policy allowing only members of the Finance?Active Directory group to access a cloud-based accounting application.
Which NGFW capability makes this policy possible?
A. Dynamic routing protocols
B. User-ID / identity integration
C. High availability clustering
D. NAT policy
Answer: B (LEAVE A REPLY)
User-ID integration maps IP addresses to authenticated users or groups, allowing identity-based security policies.

NEW QUESTION: 5
An organization is migrating its data center to Amazon Web Services (AWS) and needs to deploy VM-Series firewalls to inspect all ingress and egress traffic. The solution must provide both resilience across multiple Availability Zones and the ability to scale horizontally.
Which combination of AWS services and Palo Alto Networks components is required for this use case?
A. AWS Lambda function that monitors the firewall's health and re-routes traffic using the AWS API
B. PAN-OS active/active high availability (HA) pair with an AWS Transit Gateway
C. Amazon EC2 Auto Scaling group with VM-Series firewalls and an Amazon Gateway Load Balancer
D. Single VM-Series firewall with an Elastic IP address that can be re-associated upon failure
Answer: (SHOW ANSWER)
Using VM-Series firewalls in an EC2 Auto Scaling group provides horizontal scale-out across multiple Availability Zones, and placing them behind an Amazon Gateway Load Balancer enables resilient, distributed traffic insertion for centralized inspection of ingress and egress flows while supporting automatic scaling and failover.

NEW QUESTION: 6
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: (SHOW ANSWER)
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.

NEW QUESTION: 7
A network engineer observes a pattern of anomalous traffic hitting an external-facing zone, including a high volume of TCP packets that are not part of a new session handshake (non-SYN), and a large number of ICMP fragments. The engineer decides to apply a Zone Protection profile to mitigate these potential threats.
Which protection type within the profile must be configured?
A. Protocol Protection
B. Flood Protection

C. Reconnaissance Protection
D. Packet-Based Attack Protection
Answer: D (LEAVE A REPLY)
Packet-Based Attack Protection is specifically designed to detect and mitigate abnormal or malformed packets such as non-SYN TCP packets and ICMP fragments, which are characteristic of packet-level attacks rather than floods, reconnaissance, or protocol misuse.

NEW QUESTION: 8
A network administrator is configuring an Aggregate Ethernet (AE) interface on an active/passive high availability (HA) pair. To reduce network downtime during a failover, the administrator wants the passive firewall's AE interface to be fully negotiated with the switch before it becomes active.
Which Link Aggregation Control Protocol (LACP) setting achieves this administrator's goal?
A. LACP Mode active
B. Enable in HA passive state
C. System Priority: 1
D. Transmission Rate: fast
Answer: B (LEAVE A REPLY)
Enabling LACP in the HA passive state allows the passive firewall to negotiate and maintain the LACP session with the switch even while it is not active, so the aggregate Ethernet interface is already up and fully formed when a failover occurs, minimizing downtime.

NEW QUESTION: 9
An NGFW is deployed inline to inspect traffic without requiring any changes to existing IP addressing or routing configurations.
Which deployment mode is being used?
A. Layer 3 routed mode
B. Layer 2 switching mode
C. Virtual Wire / transparent mode
D. VPN mode
Answer: C (LEAVE A REPLY)
Virtual Wire (transparent) mode allows the NGFW to inspect traffic without modifying the network topology.

NEW QUESTION: 10
An administrator enables SSL Forward Proxy decryption using a self-signed certificate on a Palo Alto Networks firewall as the forward trust certificate. Shortly after, users report receiving "Your connection is not private" browser errors for all external websites.

What is the most likely cause of these widespread certificate errors?
A. The decryption policy is configured with a "no-decrypt" action, which causes browsers to reject the connection.
B. The external websites are using TLS 1.3, which cannot be decrypted by the firewall without a specific license.
C. The firewall's forward untrust certificate has expired, preventing it from identifying untrusted sites.
D. The firewall's self-signed CA certificate is not deployed to the trusted certificate store on client endpoints.
Answer: (SHOW ANSWER)
SSL Forward Proxy relies on the firewall acting as a trusted certificate authority. If the self-signed forward trust certificate is not installed in the trusted root certificate store of client devices, browsers will not trust the certificates generated by the firewall, resulting in widespread
"connection not private" warnings for all decrypted HTTPS sites.

NEW QUESTION: 11
In regard to the Advanced Routing Engine (ARE), what must be enabled first when configuring a logical router on a PAN-OS firewall?
A. License
B. Plugin
C. Content update
D. General setting
Answer: (SHOW ANSWER)
The Advanced Routing Engine (ARE) requires enabling its general setting as the first step before configuring any logical routers on a PAN-OS firewall.
Configuration Steps
Access Network > Routing > General and enable Advanced Routing to activate the ARE feature set, including logical router support. Only after this can logical routers be added under Network > Routing > Logical Routers.

NEW QUESTION: 12
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 (LEAVE A REPLY)
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: 13
An organization is deploying VM-Series firewalls in Microsoft Azure to secure its VNets. A key requirement is that the security infrastructure must be resilient to the failure of an entire Azure Availability Zone.
What is the recommended method to achieve this goal?
A. Deploy multiple, independent VM-Series firewalls in different Availability Zones and use an Azure Load Balancer to distribute traffic to them.
B. Implement a Terraform configuration that automatically redeploys the firewall in a new zone if the original one fails.
C. Use Azure Traffic Manager to direct traffic to a primary VM-Series firewall, with a second firewall in another zone as a failover target.
D. Configure PAN-OS active/passive high availability (HA) between two VM-Series instances in separate Availability Zones using HA links over a VNet peering connection.
Answer: A (LEAVE A REPLY)
Deploying multiple independent VM-Series firewalls across different Azure Availability Zones and placing them behind an Azure Load Balancer provides zone-level fault tolerance by design, ensuring traffic continues to flow if an entire zone fails, without relying on stateful HA dependencies or single-instance failover mechanisms.

NEW QUESTION: 14
When configuring a physical interface on a Palo Alto Networks firewall, which IP-based service is only available if the interface is set to Layer 3 mode?
A. DDNS client
B. NetFlow export
C. QoS
D. Link monitoring
Answer: B (LEAVE A REPLY)
NetFlow export requires the interface to operate in Layer 3 mode because it depends on IP routing and flow records derived from Layer 3 traffic, which are not available on interfaces configured as Layer 2, virtual wire, or other non-Layer 3 modes.

NEW QUESTION: 15
Which method creates the most reliable user-to-IP mapping due to being based on a direct authentication from the user's device to the firewall?

A. Portal authentication
B. PAN-OS XML API to push mappings
C. Polling security event logs with a User-ID agent
D. Authentication logs from Syslog receiver
Answer: (SHOW ANSWER)
Portal authentication creates user-to-IP mappings through direct, interactive authentication from the user's device to the firewall itself, making it the most reliable method because the identity is verified in real time at the source rather than inferred from logs or external systems.

NEW QUESTION: 16
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 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: B (LEAVE A REPLY)
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: 17
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 (LEAVE A REPLY)
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: 18
An 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: (SHOW ANSWER)
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.

NEW QUESTION: 19
An organization runs multiple Kubernetes clusters both on-premises and in public clouds (AWS, Azure, GCP). They want to deploy the Palo Alto Networks CN-Series NGFW to secure east-west traffic within each cluster, maintain consistent Security policies across all environments, and dynamically scale as containerized workloads spin up or down. They also plan to use a centralized Panorama instance for policy management and visibility.
Which approach meets these requirements?
A. Install standalone CN-Series instances in each cluster with local configuration 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: (SHOW ANSWER)

This approach meets all the requirements for securing east-west traffic within each Kubernetes cluster, maintaining consistent security policies across on-premises and cloud environments, and allowing for dynamic scaling of the CN-Series NGFWs as containerized workloads spin up or down. By using Kubernetes- native deployment tools (such as Helm), the CN-Series NGFWs can be deployed and scaled dynamically within each cluster. Local insertion into the service mesh or CNI ensures that the NGFW can inspect traffic at the appropriate points within the cluster.
Centralized management via Panorama ensures that security policies are uniform across both on-premises and cloud environments, providing visibility and control across all clusters.

NEW QUESTION: 20
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: A (LEAVE A REPLY)
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.

NEW QUESTION: 21
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 (LEAVE A REPLY)

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: 22

What is a key difference between OSPF and BGP when used in a Palo Alto Networks firewall?

A. BGP does not require neighbor relationships, while OSPF does

B. OSPF operates only on IPv6, while BGP is for IPv4

C. OSPF is used for internal routing, while BGP is primarily used for external routing

D. OSPF is faster than BGP in all scenarios

Answer: (SHOW ANSWER)

NEW QUESTION: 23

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

A. It is associated with an interface within a VSYS of a firewall.

B. It is a security object associated with a specific virtual router of a VSYS.

C. It is not associated with an interface; it is associated with a VSYS itself.

D. It is a security object associated with a specific VSYS.

Answer: A,D (LEAVE A REPLY)

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

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

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

NEW QUESTION: 24
An organization wants to protect its internal network from previously unknown malware that does not match any existing signatures.
Which NGFW feature BEST addresses this requirement?
A. Stateful inspection
B. Intrusion Prevention System (IPS)
C. URL filtering
D. Sandbox / Advanced Threat Protection
Answer: D (LEAVE A REPLY)
Sandboxing executes suspicious files in an isolated environment and analyzes their behavior, making it effective against zero-day threats.

NEW QUESTION: 25
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 CA. 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.
B. Distribute the root and intermediate CA certificates via Panorama as shared objects to ensure all firewalls have a consistent trust chain. Configure OCSP responder profiles on each firewall to offload revocation checks to an internal OCSP server while keeping CRL checks as a fallback.
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.
C. Configure each firewall independently to trust the root and intermediate CA certificates. 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.
D. 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. Manually

install user certificates on endpoints and synchronize firewall certificate stores through frequent manual SSH updates to maintain consistency.

Answer: B (LEAVE A REPLY)

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: 26

A firewall administrator needs to configure a new Palo Alto Networks firewall so that its management interface automatically obtains an IP address, netmask, and default gateway from the network.

Which command should be executed in the CLI to accomplish this goal?

A. set deviceconfig system interface mgt mode dhcp

B. set network interface management dhcp enable

C. set deviceconfig system type dhcp-client

D. configure system management-interface ip dynamic

Answer: (SHOW ANSWER)

This command configures the management interface to operate in DHCP mode, allowing it to automatically obtain an IP address, subnet mask, and default gateway from the network's DHCP server.

NEW QUESTION: 27

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 (LEAVE A REPLY)

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: 28
A firewall administrator uses Panorama to manage a fleet of firewalls. After successfully onboarding the firewalls to Strata Logging Service and enabling cloud logging via a template, the security operations team reports that they can no longer see new logs on the on-premises Panorama log collectors. Logs are appearing correctly in Strata Logging Service.
Which setting was likely missed in the Panorama template configuration?
A. The device certificates for the Panorama log collectors were not renewed after enabling the cloud logging connection.
B. Duplicate logging (cloud and on-premises) is disabled under Device --> Setup --> Management.
C. The Log Forwarding profile was modified to send logs only to the Strata Logging Service and no longer includes the on-premises Panorama log collectors.
D. The Panorama log collectors were not defined as primary destinations within the collector group configuration for the managed firewalls.
Answer: B (LEAVE A REPLY)
When cloud logging is enabled, logs are sent exclusively to Strata Logging Service unless duplicate logging is explicitly enabled. If duplicate logging is not enabled under Device → Setup
→ Management in the Panorama template, logs will no longer be forwarded to on-premises Panorama log collectors even though they appear correctly in Strata Logging Service.

NEW QUESTION: 29
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 (LEAVE A REPLY)
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: 30
When multiple routes have the same destination prefix, which attribute does the firewall use first to determine route preference?
A. Administrative distance
B. Route metric
C. Next-hop availability
D. Longest prefix match
Answer: D (LEAVE A REPLY)
When multiple routes exist, the firewall first applies longest prefix match, meaning the route with the most specific destination prefix is selected before considering any other attributes such as administrative distance or metric.

NEW QUESTION: 31
In a Collector Group with multiple Log Collectors, enabling redundancy ensures that:
A. Each log is stored only on the primary Log Collector.
B. Each log has two copies, each residing on a different Log Collector.
C. Logs are distributed based on a round-robin mechanism.
D. Logs are stored in a compressed format to save space.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Before upgrading a Palo Alto Networks firewall to a new PAN-OS version, which preliminary step is crucial to ensure a smooth upgrade process?
A. Disable High Availability (HA) if configured.
B. Back up the current configuration.
C. Disable all security policies.
D. Reset the firewall to factory settings.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
When creating a Log Forwarding profile on a PAN-OS firewall to direct logs to various external and internal systems, which set of methods is available?
A. Syslog, Panorama, SD-WAN
B. Panorama/Cloud logging, email, Syslog
C. Email, Syslog, NetFlow
D. HTTP, RADIUS, SNMP
Answer: B (LEAVE A REPLY)
Log Forwarding profiles in PAN-OS support forwarding logs to Panorama or cloud logging services, sending notifications via email, and exporting logs to external systems using Syslog, which together form the supported log forwarding mechanisms for centralized management and integration.

NEW QUESTION: 34
A government agency needs to ensure that all user web access is explicitly mediated and authenticated. The agency has the following requirements:
- Client browsers must be manually configured to send traffic to the firewall's IP address and a specific port.
- The firewall must support seamless single sign-on (SSO) with the users' existing Active Directory credentials.
Which feature set should the engineer configure to meet the agency's requirements?
A. Web proxy in explicit mode with an Authentication policy by using Kerberos
B. Decryption policy that redirects users to a SAML identity provider for authentication
C. Web proxy in transparent mode with an Authentication policy by using multi-factor authentication (MFA)
D. User-ID agent integration with Authentication Portal for authentication
Answer: (SHOW ANSWER)
Explicit web proxy mode requires client browsers to be manually configured to send traffic to the firewall's IP address and port, and integrating it with an Authentication policy using

Kerberos enables seamless single sign-on with Active Directory credentials through native domain authentication without additional user interaction.

NEW QUESTION: 35
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 (LEAVE A REPLY)
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: 36
A network engineer observes that after a primary link recovers, the firewall immediately switches traffic back from the backup static route to the primary static route. The engineer checks the path monitoring configuration for the primary route.
Which value is configured for the preemptive hold time to cause this behavior?
A. Lowest possible value greater than 0
B. 0
C. Default value
D. Feature disabled
Answer: B (LEAVE A REPLY)
A preemptive hold time of 0 causes the firewall to immediately switch traffic back to the primary static route as soon as the monitored path is restored, resulting in instant failback without any delay.

NEW QUESTION: 37
What is the primary use case for the CN-Series NGFW?
A. Protecting mobile users and remote branch offices (east-west)
B. Providing security for physical data center perimeters (north-south)
C. Securing traffic in and out of a public cloud VPC or VNet (north-south)
D. Enforcing Security policies between pods in a Kubernetes environment (east-west)
Answer: D (LEAVE A REPLY)

The CN-Series NGFW is designed specifically for Kubernetes and containerized environments to enforce security policies between pods and services, providing east-west traffic inspection and control within the cluster using a container-native firewall architecture.

NEW QUESTION: 38
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 (LEAVE A REPLY)
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: 39
A network security engineer wants to create Security policy rules that allow or deny traffic based on a user's department, which corresponds to groups in the company's Active Directory. To achieve this, the firewall needs to retrieve group information from the directory server.
Which configuration object must be created first to establish the connection with the Active Directory server?
A. LDAP server profile
B. User-ID agent service account
C. Authentication sequence
D. Kerberos server profile
Answer: A (LEAVE A REPLY)
An LDAP server profile must be created first because it defines the connection parameters to the Active Directory server, enabling the firewall to query directory services and retrieve user and group information required for group-based policy enforcement.

NEW QUESTION: 40
An engineer is configuring a GlobalProtect portal and wants to enable split tunneling. The requirement is to route DNS queries for "https://www.google.com/search?q=corp.internal.com" to the DNS servers assigned by the VPN, while allowing all other DNS queries to be resolved by the client's locally configured DNS.

What is the effect of configuring this split DNS policy?
A. It provides selective DNS resolution, with specified domains resolved through the tunnel, optimizing performance for other lookups.
B. It blocks access to all domains that are not explicitly listed in the split tunnel configuration.
C. It forces all applications to use the corporate DNS servers, regardless of the split tunnel settings for IP traffic.
D. It creates a DNS proxy on the client endpoint that forwards all queries to the firewall for inspection.
Answer: A (LEAVE A REPLY)
Split DNS configuration enables selective DNS routing where only queries for specified internal domains are sent through the VPN tunnel to corporate DNS servers, while all other DNS requests continue to use the client's local DNS, optimizing performance and preserving local internet resolution.

NEW QUESTION: 41
An organization must secure its AWS and Azure environments using a managed Palo Alto Networks solution, and all policies must be synchronized from an existing Panorama deployment.
The organization wants to insert security with the least possible impact on its application teams and use existing hub-and-spoke network designs.
- The AWS environment uses a centralized AWS Transit Gateway (TGW) architecture.
- The Azure environment uses a Virtual WAN (vWAN) hub.
Which two actions are the most appropriate in this use case? (Choose two.)
A. Deploy Cloud NGFW endpoints in every application virtual private cloud (VPC), ignoring the TGW.
B. Deploy Cloud NGFW into the vWAN hub as a trusted security partner, and update routing policies to secure traffic.
C. Deploy individual VM-Series firewalls in each spoke virtual network (VNet) and manage them as a device group in Panorama.
D. Deploy Cloud NGFW endpoints into a security virtual private cloud (VPC), and adjust the TGW route tables to inspect traffic flowing though the hub.
Answer: B,D (LEAVE A REPLY)
In Azure, integrating Cloud NGFW into the Virtual WAN hub as a trusted security partner enables centralized inspection in the hub-and-spoke design while keeping spoke VNets largely unchanged. In AWS, deploying Cloud NGFW endpoints in a dedicated security VPC and steering traffic through them by updating Transit Gateway route tables provides centralized security insertion that can be driven by existing Panorama-managed policy.

NEW QUESTION: 42

How does a Palo Alto Networks firewall choose the best route when it receives routes for the same destination from different routing protocols?
A. The route that was received first will be entered into the forwarding table, and all subsequent routes will be rejected.
B. It will attempt to load balance the traffic across all routes.
C. It compares the administrative distance and chooses the one with the highest value.
D. It compares the administrative distance and chooses the one with the lowest value.
Answer: (SHOW ANSWER)
When a Palo Alto Networks firewall receives routes for the same destination from different routing protocols, it uses the administrative distance (AD) to determine the best route. The administrative distance is a measure of the trustworthiness of a route, with a lower value indicating higher preference. The firewall will choose the route with the lowest administrative distance to populate its forwarding table.

NEW QUESTION: 43
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: C,D (LEAVE A REPLY)
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: 44

An NGFW engineer is configuring multiple Layer 2 interfaces on a Palo Alto Networks firewall, and all interfaces must be assigned to the same VLAN. During initial testing, it is reported that clients located behind the various interfaces cannot communicate with each other.
Which action taken by the engineer will resolve this issue?
A. Configure each interface to belong to the same Layer 2 zone and enable IP routing between them.
B. Assign each interface to the appropriate Layer 2 zone and configure a policy that allows traffic within the VLAN.
C. Assign each interface to the appropriate Layer 2 zone and configure Security policies for interfaces not assigned to the same zone.
D. Enable IP routing between the interfaces and configure a Security policy to allow traffic between interfaces within the VLAN.
Answer: B (LEAVE A REPLY)
In a Layer 2 configuration, interfaces are typically grouped into the same Layer 2 zone. When the interfaces are assigned to the same VLAN, the firewall will treat them as part of the same broadcast domain.
In a Layer 2 setup, interfaces must be in the same Layer 2 zone to allow the traffic within the same VLAN to pass. Additionally, a security policy must be configured to allow traffic within this VLAN or zone. This will resolve the issue by ensuring that traffic is permitted between clients behind different interfaces assigned to the same VLAN.

NEW QUESTION: 45
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 (LEAVE A REPLY)
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: 46
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. 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: (SHOW ANSWER)

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: 47

What is a valid configurable limit for setting resource quotas when defining a new VSYS on a Palo Alto Networks firewall?

A. Percentage of total CPU utilization

B. Maximum number of SSL decryption rules
C. Maximum number of virtual routers
D. Disk space allocation for logs
Answer: B (LEAVE A REPLY)
When defining a new VSYS, PAN-OS allows administrators to set explicit resource quotas on policy-related objects, including limits on rule capacities, which can include SSL decryption rules as part of security policy resources, enabling controlled allocation of configuration and processing capacity per VSYS.

NEW QUESTION: 48
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: A (LEAVE A REPLY)
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.

NEW QUESTION: 49
A network security engineer is segmenting a single firewall into VSYS-A and VSYS-B. For traffic to flow from VSYS-A to VSYS-B, external zones are required.
What are two fundamental properties of the external zones needed for this configuration? (Choose two.)
A. They must be linked to the same virtual router as the ingress interface.
B. They represent their parent VSYS without being tied to a physical or logical interface.
C. They are a security construct belonging to a single VSYS.
D. They are automatically created when inter-VSYS routing is enabled.
Answer: B,C (LEAVE A REPLY)
External zones act as logical representations of another VSYS and are not bound to any physical or logical interface, enabling inter-VSYS traffic flow, and they are security objects that belong to a single VSYS, allowing security policy enforcement between VSYS contexts.

NEW QUESTION: 50

Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?

A. DDNS

B. Link Duplex

C. NetFlow

D. LLDP

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 51

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 (LEAVE A REPLY)

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: 52

What are two valid zone types that can be selected from the zone configuration menu, per Palo Alto Networks best practices? (Choose two.)

A. Layer 3

B. Layer 2

C. Management

D. DMZ

Answer: (SHOW ANSWER)

Layer 3 and Layer 2 are valid, configurable zone types in PAN-OS and are standard zone constructs used to define traffic segmentation and policy enforcement boundaries on the firewall.

NEW QUESTION: 53
An organization requires a single security platform that integrates firewalling, VPN, intrusion prevention, and malware protection to simplify operations.
Which security concept BEST describes this approach?
A. Defense in depth
B. Unified Threat Management / NGFW
C. Network micro-segmentation
D. Zero Trust Architecture
Answer: B (LEAVE A REPLY)
NGFWs and UTM platforms combine multiple security functions into a single device, reducing complexity and improving manageability.

NEW QUESTION: 54
An organization uses Cloud Identity Engine (CIE) to gather user information from its on-premises Active Directory (AD) for employees and a separate Azure AD for external partners. Due to compliance regulations, the firewalls protecting the internal network must not have any identity information about external partners. Conversely, firewalls in the partner-facing DMZ should only be aware of partner identities.
Which CIE feature is designed to solve this data partitioning requirement?
A. Panorama templates, which can be used to push different User-ID agent configurations to each firewall group
B. Segments, which can be configured to create distinct, filter-based views of users and groups that are then redistributed only to the appropriate firewalls
C. Multiple tenants, where a separate CIE tenant is required for each user directory to maintain isolation
D. Directory sync filtering, which is used at the source to prevent specific OUs from being imported into CIE
Answer: B (LEAVE A REPLY)
Segments in Cloud Identity Engine allow administrators to create filtered, logical partitions of identity data and redistribute only the relevant users and groups to specific firewalls, ensuring strict separation of employee and partner identities in compliance-driven environments.

NEW QUESTION: 55
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: (SHOW ANSWER)
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: 56
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 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: B (LEAVE A REPLY)
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: 57
An administrator is configuring a site-to-site IPSec VPN and assigns an IP address to the tunnel interface.

Which two abilities are enabled by this specific configuration step? (Choose two.)
A. Configuring tunnel monitoring to verify the liveliness of the connection.
B. Firewall performing NAT traversal.
C. Running a dynamic routing protocol like OSPF over the tunnel.
D. Firewall encrypting and decrypting packet payloads.
Answer: A,C (LEAVE A REPLY)
Assigning an IP address to the tunnel interface allows the firewall to perform tunnel monitoring by sourcing and receiving keepalive traffic over the tunnel, and enables the use of dynamic routing protocols such as OSPF across the tunnel because the tunnel interface becomes a routable Layer 3 interface.

NEW QUESTION: 58
How do Zone Protection Profiles enhance network security?
A. By providing protection against flood attacks, reconnaissance scans, and packet-based threats
B. By replacing security policies with predefined rule sets
C. By dynamically assigning users to security groups
D. By encrypting all traffic entering and leaving the zone
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
A cloud security team wants to extend its existing Palo Alto Networks Security policies into the organization's Kubernetes environments. The team requires an NGFW solution that can be deployed natively as a container and managed by Panorama.
Which firewall form factor meets these requirements?
A. Cloud NGFW
B. PA-5400 Series
C. VM-Series
D. CN-Series
Answer: D (LEAVE A REPLY)
The CN-Series firewall is a container-native NGFW designed specifically for Kubernetes environments, deployable as containers and fully manageable by Panorama, enabling consistent policy enforcement across cloud-native and traditional network environments.

NEW QUESTION: 60
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: B (LEAVE A REPLY)
In PAN-OS service route configuration, IPSec tunnel-related traffic (such as IKE/IPSec control- plane communication) is, by default, sourced from the management interface unless explicitly overridden.
This includes:
- IKE negotiation traffic
- IPSec tunnel establishment and maintenance traffic

NEW QUESTION: 61
Which configuration in the LACP tab will enable pre-negotiation for an Aggregate Ethernet (AE) interface on a Palo Alto Networks high availability (HA) active/passive pair?
A. Set Transmission Rate to "fast."
B. Set passive link state to "Auto."
C. Set "Enable in HA Passive State."
D. Set LACP mode to "Active."
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 62
An automation engineer is developing a Python script to standardize SD-WAN deployments across multiple customer tenants in Panorama. A key requirement is to programmatically create path quality profiles to monitor link performance based on latency, jitter, and packet loss.
Which API call is required for this task?
A. XML API command with an xpath of config/devices/entry/vsys/entry/path-quality-profiles on Panorama
B. XML API command with an xpath of sdwan/path-quality-profiles on a managed firewall

C. POST request to the SDWanPathQualityProfiles object endpoint via the REST API on Panorama
D. POST request to the pathMonitoringProfiles object endpoint via the REST API on a managed firewall
Answer: C (LEAVE A REPLY)
Path quality profiles for SD-WAN are created and managed centrally in Panorama using the REST API, and the SDWanPathQualityProfiles object endpoint is specifically designed to programmatically define latency, jitter, and packet-loss thresholds for SD-WAN monitoring across multiple tenants and devices.