Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

NEW QUESTION 1
An enterprise uses GlobalProtect with both user- and machine-based certificate authentication and requires pre-logon, OCSP checks, and minimal user disruption. They manage multiple firewalls via Panorama and deploy domain-issued machine certificates via Group Policy.
Which approach ensures continuous, secure connectivity and consistent policy enforcement?

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

Answer: B

Explanation:
To ensure continuous, secure connectivity and consistent policy enforcement with GlobalProtect in an enterprise environment that uses user- and machine-based certificate authentication, the approach should:
Distribute root and intermediate CAs via Panorama templates: This ensures that all firewalls managed by Panorama share the same trusted certificate authorities for consistency and security.
Use distinct certificate profiles for user vs. machine certificates: This enables separate handling of user and machine authentication, ensuring that both types of certificates are managed and validated appropriately.
Reference an internal OCSP responder: By integrating OCSP checks, the firewall can validate certificate revocation in real-time, meeting the security requirement while minimizing the overhead and latency associated with traditional CRLs (Certificate Revocation Lists).
Automate certificate deployment with Group Policy: This ensures that machine certificates are deployed in a consistent and scalable manner across the enterprise, reducing manual intervention and minimizing user disruption.
This approach supports the requirements for pre-logon, OCSP checks, and minimal user disruption, while maintaining a secure, automated, and consistent authentication process across all firewalls managed via Panorama.

NEW QUESTION 2
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 onl
B. Export daily policy configuration snapshots to Panorama for recordkeeping, but do not unify policy enforcement.
C. Configure the CN-Series only in public cloud clusters, and rely on Kubernetes Network Policies for on-premises cluster securit
D. Synchronize partial policy information into Panorama manually as needed.
E. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in eachcluster, ensuring local insertion into the service mesh or CN
F. Manage all CN-Series firewalls centrally from Panorama, applying uniform Security policies across on-premises and cloud clusters.
G. Deploy a single CN-Series firewall in the on-premises data center to process traffic for all clusters, connecting remote clusters via VPN or peerin
H. Manage this single instance through Panorama.

Answer: C

Explanation:
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 3
An NGFW engineer is configuring multiple Panorama-managed firewalls to start sending all logs to Strata Logging Service. The Strata Logging Service instance has been provisioned, the required device certificates have been installed, and Panorama and the firewalls have been successfully onboarded to Strata Logging Service.
Which configuration task must be performed to start sending the logs to Strata Logging Service and continue forwarding them to the Panorama log collectors as well?

A. Modify all active Log Forwarding profiles to select the ??Cloud Logging?? option in each profile match list in the appropriate device groups.
B. Enable the ??Panorama/Cloud Logging?? option in the Logging and Reporting Settings section under Device --> Setup --> Management in the appropriate templates.
C. Select the ??Enable Duplicate Logging?? option in the Cloud Logging section under Device--> Setup --> Management in the appropriate templates.
D. Select the ??Enable Cloud Logging?? option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.

Answer: D

Explanation:
To begin sending logs to Strata Logging Service while continuing to forward them to Panorama log collectors, the necessary configuration is to enable Cloud Logging. This option is configured in the Cloud Logging section under Device Setup Management in the appropriate templates. Once enabled, this ensures that logs are directed both to the Strata Logging Service (cloud) and to the Panorama log collectors.

NEW QUESTION 4
According to dynamic updates best practices, what is the recommended threshold value for content updates in a mission- critical network?

A. 8 hours

B. 16 hours
C. 32 hours
D. 48 hours

Answer: A

Explanation:
For a mission-critical network, it is recommended to configure the content update threshold to 8 hours. This ensures that the network is protected with the latest threat intelligence, updates to signatures, and other critical content, minimizing the exposure to newly discovered vulnerabilities and threats.
Regular content updates are crucial in mission-critical environments to ensure the firewall is up-to-date with the latest protections. 8 hours is considered an optimal balance between timely updates and network performance.

NEW QUESTION 5
Which zone type allows traffic between zones in different virtual systems (VSYS), without the traffic leaving the firewall?

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

Answer: B

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

NEW QUESTION 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: D

Explanation:
Server monitoring is the most reliable method for mapping users to IP addresses in PAN- OS. This method allows the firewall to monitor specific servers, such as Microsoft Active Directory (AD) or LDAP servers, to dynamically retrieve and update user-to-IP mappings. It provides a more accurate and up-to-date mapping of users to their associated IP addresses, as it directly queries user databases in real time.

NEW QUESTION 7
Which configuration step is required when implementing a new self-signed root certificate authority (CA) certificate for SSL decryption on a Palo Alto Networks firewall?

A. Import the new subordinate CA certificate into the trust stores of all client devices.
B. Set the subordinate CA certificate as the default routing certificate for all network traffic.
C. Configure the subordinate CA to issue certificates with indefinite validity periods.
D. Disable all existing SSL decryption rules until the new certificate is fully propagated.

Answer: A

Explanation:
When implementing a new self-signed root certificate authority (CA) for SSL decryption on a Palo Alto Networks firewall, the subordinate CA certificate (which is generated by the firewall) must be imported into the trust stores of all client devices. This ensures that client devices trust the firewall as a valid certificate authority, enabling the firewall to decrypt and re-encrypt SSL traffic.
Importing the subordinate CA certificate into the client devices' trust stores is necessary for those devices to trust the new self-signed root CA and properly handle SSL decryption traffic.

NEW QUESTION 8
When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

A. Service graph
B. Ansible automation modules
C. Panorama role-based access control
D. CN-Series firewalls

Answer: D

Explanation:
When integrating Kubernetes with Palo Alto Networks NGFWs, the CN-Series firewalls are specifically designed to secure traffic between microservices in containerized environments. These firewalls provide advanced security features like Application Identification (App-ID), URL filtering, and Threat Prevention to secure communication between containers and microservices within a Kubernetes environment.

NEW QUESTION 9
An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The

application will be able to make any approved changes directly to devices via API.
What is a requirement for the application to create SD-WAN interfaces?

A. REST API??s ??sdwanInterfaceprofiles?? parameter on a Panorama device
B. REST API??s ??sdwanInterfaces?? parameter on a firewall device
C. XML API??s ??sdwanprofiles/interfaces?? parameter on a Panorama device
D. XML API??s ??InterfaceProfiles/sdwan?? parameter on a firewall device

Answer: B

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

NEW QUESTION 10
Which type of firewall resource can be assigned when configuring a new firewall virtual system (VSYS)?

A. ICPU
B. Sessions limit
C. Memory
D. Security profile limit

Answer: B

Explanation:
When configuring a new firewall virtual system (VSYS) on a Palo Alto Networks firewall, one of the resources that can be assigned is the sessions limit. This setting allows the administrator to control the number of active sessions that can be handled by the VSYS, ensuring that each virtual system has an appropriate allocation of resources based on its needs.

NEW QUESTION 10
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: A

Explanation:
To enable the Advanced Routing Engine (ARE) on a Palo Alto Networks firewall, the license for the ARE must be applied first. Without the proper license, the firewall cannot activate and use the advanced routing features provided by ARE, such as support for more complex routing protocols (e.g., BGP, OSPF, etc.). Once the license is applied and validated, the routing engine can be configured, allowing the creation of logical routers and routing policies.

NEW QUESTION 12
For which two purposes is an IP address configured on a tunnel interface? (Choose two.)

A. Use of dynamic routing protocols
B. Tunnel monitoring
C. Use of peer IP
D. Redistribution of User-ID

Answer: AB

Explanation:
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.

NEW QUESTION 14
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

Explanation:
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 18
What is a result of enabling split tunneling in the GlobalProtect portal configuration with the ??Both Network Traffic and DNS?? option?

A. It specifies when the secondary DNS server is used for resolution to allow access to specific domains that are not managed by the VPN.
B. It allows users to access internal resources when connected locally and external resources when connected remotely using the same FQDN.
C. It allows devices on a local network to access blocked websites by changing which DNS server resolves certain domain names.
D. It specifies which domains are resolved by the VPN-assigned DNS servers and which domains are resolved by the local DNS servers.

Answer: D

Explanation:
When split tunneling is enabled with the "Both Network Traffic and DNS" option in the GlobalProtect portal configuration, it allows the firewall to control which traffic is sent over the VPN tunnel and which is not. Specifically, it determines which domains are resolved by the VPN-assigned DNS servers (for domains requiring VPN access) and which are resolved by local DNS servers (for domains that can be accessed without the VPN tunnel).

NEW QUESTION 22
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: C

Explanation:
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 25
What are the phases of the Palo Alto Networks AI Runtime Security: Network Intercept solution?

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

Answer: B

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

NEW QUESTION 29
During an upgrade to the routing infrastructure in a customer environment, the network administrator wants to implement Advanced Routing Engine (ARE) on a Palo Alto Networks firewall.
Which firewall models support this configuration?

A. PA-5280, PA-7080, PA-3250, VM-Series
B. PA-455, VM-Series, PA-1410, PA-5450
C. PA-3260, PA-5410, PA-850, PA-460
D. PA-7050, PA-1420, VM-Series, CN-Series

Answer: C

Explanation:
The Advanced Routing Engine (ARE) is supported on Palo Alto Networks firewalls that utilize the PAN-OS 11.0+ software and have the required hardware architecture. The supported models include PA-3200 Series, PA-5400 Series, PA-800 Series, and PA-400 Series. These models provide enhanced routing capabilities, including BGP, OSPF, and more complex routing policies.
PA-3260 and PA-5410 are part of the PA-3200 and PA-5400 Series, which are known to support ARE.
PA-850 and PA-460 are within the PA-800 and PA-400 Series, which also support ARE

NEW QUESTION 32
In a hybrid cloud deployment, what is the primary function of Ansible in managing Palo Alto Networks NGFWs?

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

Answer:

D

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

NEW QUESTION 34
Which CLI command is used to configure the management interface as a DHCP client?

A. set network dhcp interface management
B. set network dhcp type management-interface
C. set deviceconfig system type dhcp-client
D. set deviceconfig management type dhcp-client

Answer: D

Explanation:
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.

NEW QUESTION 38
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 orreissue 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

Explanation:
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 42
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NGFW-Engineer Practice Exam Features:

* NGFW-Engineer Questions and Answers Updated Frequently

* NGFW-Engineer Practice Questions Verified by Expert Senior Certified Staff

* NGFW-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NGFW-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year