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
Which statement describes the role of Terraform in deploying Palo Alto Networks NGFWs?

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

Answer: C

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

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

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

Answer: B

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

NEW QUESTION 4
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: D

Explanation:
By default, the Autonomous Digital Experience Manager (ADEM) traffic is configured to use the management interface in a Palo Alto Networks firewall. The management interface is typically used for management-related traffic, such as monitoring and logging, and it is configured to handle ADEM-related traffic for the optimal performance of digital experience monitoring features.
This default configuration helps ensure that ADEM traffic does not interfere with regular traffic that may traverse other interfaces, such as traffic from security

zones or IPSec tunnels.

NEW QUESTION 5
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 6
Which 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: D

Explanation:
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.

NEW QUESTION 7
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: D

Explanation:
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 8
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 9
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

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.

NEW QUESTION 10
Which two zone types are valid when configuring a new security zone? (Choose two.)

A. Tunnel
B. Intrazone
C. Internal
D. Virtual Wire

Answer: AD

Explanation:
When configuring a new security zone on a Palo Alto Networks firewall, the two valid zone types are:
Tunnel: A Tunnel zone is used for traffic that is associated with a VPN tunnel, such as IPSec tunnels. Traffic passing through a tunnel interface is classified into this zone.
Virtual Wire: A Virtual Wire zone is used when a firewall operates in transparent mode (also known as Layer 2 mode). In this configuration, the firewall can inspect traffic without modifying the IP address structure of the network.

NEW QUESTION 10
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 C
B. 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.
C. Distribute the root and intermediate CA certificates via Panorama as shared objects to ensure all firewalls have a consistent trust chai
D. Configure OCSP responder profiles oneach firewall to offload revocation checks to an internal OCSP server while keeping CRL checks as a fallbac
E. 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.
F. Configure each firewall independently to trust the root and intermediate CA certificate
G. 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.
H. Obtain wildcard certificates from a public CA for both user and device authentication, and configure firewalls to perform CRL polling at the default update interva
I. Manually install user certificates on endpoints and synchronize firewall certificate stores through frequent manual SSH updates to maintain consistency.

Answer: B

Explanation:
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 12
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 16
Without performing a context switch, which set of operations can be performed that will affect the operation of a connected firewall on the Panorama GUI?

A. Restarting the local firewall, running a packet capture, accessing the firewall CLI
B. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostname
C. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network Profile
D. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reports

Answer: B

Explanation:
In Panorama, without performing a context switch, the administrator can perform local configuration tasks directly on the connected firewall. The following operations can be done:
Modification of local security rules: Security rules can be modified directly on the connected firewall from the Panorama GUI.
Modification of a Layer 3 interface: Changes to the Layer 3 interfaces on the connected firewall can be done from Panorama, without needing to switch to the firewall's local interface.
Modification of the firewall device hostname: The firewall's hostname can be changed via Panorama.

NEW QUESTION 19
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 24
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: C

Explanation:
In a High Availability (HA) active/passive pair configuration, when setting up an Aggregate Ethernet (AE) interface, enabling the "Enable in HA Passive State" option allows the interface to participate in LACP (Link Aggregation Control Protocol) even when the system is in the passive state. This ensures that the pre-negotiation of the LACP link occurs, allowing the link aggregation to be ready as soon as the firewall becomes active.

NEW QUESTION 27
How does a Palo Alto Networks NGFW respond when the preemptive hold time is set to 0 minutes during configuration of route monitoring?

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

Answer: D

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

NEW QUESTION 30
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 31
Which forwarding methods can be used on the Objects tab when configuring the Log Forwarding profile?

A. Panorama, syslog, email
B. Syslog, HTTP, NetFlow

C. Panorama, ADEM, syslog
D. SNMP, HTTP, RADIUS

Answer: A

Explanation:
When configuring the Log Forwarding profile on a Palo Alto Networks firewall, the forwarding methods available include:
Panorama: For forwarding logs to a Panorama management system. Syslog: For forwarding logs to a syslog server.
Email: For sending logs via email.

NEW QUESTION 36
.....

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