Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

NEW QUESTION 1
When configuring a Zone Protection profile, in which section (protection type) would an NGFW engineer configure options to protect against activities such as spoofed IP addresses and split handshake session establishment attempts?

A. Flood Protection
B. Protocol Protection
C. Packet-Based Attack Protection
D. Reconnaissance Protection

Answer: B

Explanation:
In the context of a Zone Protection profile, Protocol Protection is the section used to configure protections against activities such as spoofed IP addresses and split handshake session establishment attempts. These types of attacks typically involve manipulating protocol behaviors, such as IP address spoofing or session hijacking, and are mitigated by the Protocol Protection settings.

NEW QUESTION 2
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 3
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 4
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 5
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 6
An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logon stage and SAML-based multi-factor authentication (MFA) for user logon.
How does the GlobalProtect agent process the authentication flow on Windows endpoints?

A. The GlobalProtect agent uses the machine certificate to establish a pre-logon tunnel; upon user sign-in, it prompts for SAML-based MFA credentials, ensuring both device and user identities are validated before granting full access.
B. The GlobalProtect agent uses the machine certificate during pre-logon for initial tunnel establishment, and then seamlessly reuses the same machine certificate for user-based authentication without requiring MFA.
C. Once the machine certificate is validated at pre-logon, the Windows endpoint completes MFA on behalf of the user by passing existing Windows Credential Provider details to the GlobalProtect gateway without prompting the user.
D. GlobalProtect requires the user to log in first for SAML-based MFA before establishing the pre-logon tunnel, rendering the pre-logon certificate authentication (CA) flow redundant.

Answer: A

Explanation:
In a hybrid authentication model with both certificate-based authentication for pre-logon and SAML-based multi-factor authentication (MFA) for user logon, the GlobalProtect agent processes the flow as follows:
During the pre-logon stage, the agent uses the machine certificate to authenticate and establish the initial VPN tunnel.
Once the user logs in (after the machine is connected), the agent then triggers SAML- based MFA to ensure the user is authenticated with multi-factor authentication, validating both the device and the user identity before granting full access.
This method ensures that both the device and user are properly authenticated and validated in the hybrid authentication model.

NEW QUESTION 7
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 8
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 9
Palo Alto Networks NGFWs use SSL/TLS profiles to secure which two types of connections? (Choose two.)

A. NAT tables
B. User Authentication
C. GlobalProtect Gateways
D. GlobalProtect Portal

Answer: CD

Explanation:
Palo Alto Networks Next-Generation Firewalls (NGFWs) use SSL/TLS profiles to secure connections for services such as GlobalProtect Gateways and GlobalProtect Portals. These profiles are used to manage the SSL/TLS encryption and decryption for secure communication between the firewall and clients (such as VPN clients for GlobalProtect). This helps ensure the confidentiality and integrity of the data during transmission.

NEW QUESTION 10
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 10
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 15
Which set of options is available for detailed logs when building a custom report on a Palo Alto Networks NGFW?

A. Traffic, User-ID, URL
B. Traffic, threat, data filtering, User-ID
C. GlobalProtect, traffic, application statistics
D. Threat, GlobalProtect, application statistics, WildFire submissions

Answer: B

Explanation:

When building a custom report on a Palo Alto Networks NGFW, you can select detailed logs that provide specific insights into various aspects of firewall activity. The available options for detailed logs typically include:
Traffic logs: These provide information on the network traffic passing through the firewall. Threat logs: These logs capture data related to identified security threats, such as malware or intrusion attempts.
Data filtering logs: These logs capture events related to data filtering policies, such as preventing the transfer of sensitive data.
User-ID logs: These logs associate user identities with the traffic and activities observed on the firewall, enabling user-based policy enforcement.

NEW QUESTION 20
.....

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