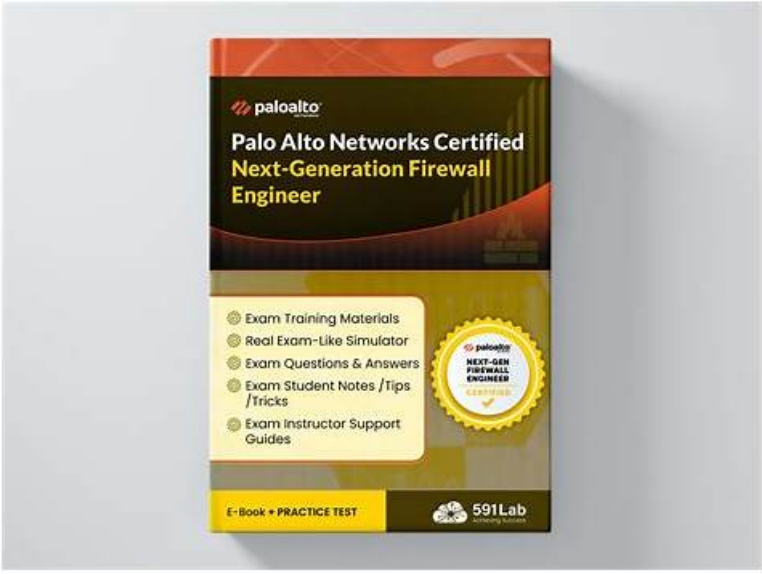
100% Pass High Hit-Rate Palo Alto Networks - Premium NGFW-Engineer Exam



P.S. Free 2026 Palo Alto Networks NGFW-Engineer dumps are available on Google Drive shared by Exam4Tests: https://drive.google.com/open?id=19WEF0B7-RSWewAM126Jdj33gkjeK-ly9

As you can see from the demos that on our website that our NGFW-Engineer practice engine have been carefully written, each topic is the essence of the content. Only should you spend about 20 - 30 hours to study NGFW-Engineer preparation materials carefully can you take the exam. The rest of time you can go to solve all kinds of things in life, ensuring that you don't delay both study and work. Our NGFW-Engineer Exam Braindumps will save your time, money and efforts to success.

Palo Alto Networks NGFW-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Integration and Automation: This section measures the skills of Automation Engineers in deploying and managing Palo Alto Networks NGFWs across various environments. It includes the installation of PA-Series, VM-Series, CN-Series, and Cloud NGFWs. The use of APIs for automation, integration with third-party services like Kubernetes and Terraform, centralized management with Panorama templates and device groups, as well as building custom dashboards and reports in Application Command Center (ACC) are key topics.
Topic 2	• PAN-OS Device Setting Configuration: This section evaluates the expertise of System Administrators in configuring device settings on PAN-OS. It includes implementing authentication roles and profiles, and configuring virtual systems with interfaces, zones, routers, and inter-VSYS security. Logging mechanisms such as Strata Logging Service and log forwarding are covered alongside software updates and certificate management for PKI integration and decryption. The section also focuses on configuring Cloud Identity Engine User-ID features and web proxy settings.
Topic 3	• PAN-OS Networking Configuration: This section of the exam measures the skills of Network Engineers in configuring networking components within PAN-OS. It covers interface setup across Layer 2, Layer 3, virtual wire, tunnel interfaces, and aggregate Ethernet configurations. Additionally, it includes zone creation, high availability configurations (active • active and active • passive), routing protocols, and GlobalProtect setup for portals, gateways, authentication, and tunneling. The section also addresses IPSec, quantum-resistant cryptography, and GRE tunnels.

>> Premium NGFW-Engineer Exam <<

Pass Guaranteed Latest NGFW-Engineer - Premium Palo Alto Networks Next-Generation Firewall Engineer Exam

Our NGFW-Engineer exam questions just focus on what is important and help you achieve your goal. When the reviewing process gets some tense, our NGFW-Engineer practice materials will solve your problems with efficiency. With high-quality NGFW-Engineer Guide materials and flexible choices of learning mode, they would bring about the convenience and easiness for you. Every page is carefully arranged by our experts with clear layout and helpful knowledge to remember.

Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q57-Q62):

NEW QUESTION # 57
After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish. Which of the following actions will resolve this issue?

- A. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.
- B. Check that IPSec is enabled in the management profile on the external interface.
- C. Configure the Proxy IDs to match the Cisco ASA configuration.
- D. Validate the tunnel interface VLAN against the peer's configuration.

Answer: C

Explanation:
The Proxy IDs (or Traffic Selectors) define the local and remote subnets that are allowed to communicate over the IPSec tunnel. If the Proxy IDs on the Palo Alto Networks firewall do not match the configuration on the Cisco ASA, the tunnel will fail to establish because the firewalls won't agree on which traffic to encrypt. Ensuring that the Proxy IDs match between the Palo Alto Networks firewall and the Cisco ASA will resolve the issue.

NEW QUESTION # 58
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. Packet-Based Attack Protection
- C. Flood Protection
- D. Reconnaissance Protection

Answer: B

Explanation:
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 # 59
What is a result of enabling split tunneling in the GlobalProtect portal configuration with the "Both Network Traffic and DNS" option?

- A. It allows users to access internal resources when connected locally and external resources when connected remotely using the same FQDN.
- B. It specifies when the secondary DNS server is used for resolution to allow access to specific domains that are not managed by the VPN.
- C. It specifies which domains are resolved by the VPN-assigned DNS servers and which domains are resolved by the local

DNS servers.

- D. It allows devices on a local network to access blocked websites by changing which DNS server resolves certain domain names.

Answer: C

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 # 60
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. Configure a single certificate profile for both user and machine certificates. Rely solely on CRLs for revocation to minimize complexity.
- B. Deploy self-signed certificates on each firewall, allow IP-based authentication to override certificate checks, and use default GlobalProtect settings for user / machine identification.
- C. 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.
- D. Use a wildcard certificate from a public CA, disable all revocation checks to reduce latency, and manage certificate renewals manually on each firewall.

Answer: C

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 # 61
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 and add the "SAML Identity Provider" Server Profile to the authentication profile for the "RADIUS" Server Profile.
- B. Create a testing and rollback plan for the transition from Radius to SAML, as the two authentication profiles cannot be run in tandem.
- C. Create an authentication sequence that includes both the "RADIUS" Server Profile and "SAML Identity Provider" Server Profile to run the two services in tandem.
- D. Create and apply an authentication profile with the "SAML Identity Provider" Server Profile.

Answer: A,C

Explanation:
To enable both RADIUS and SAML authentication to run in parallel during the transition period, you need to configure an authentication sequence and an authentication profile that includes both authentication methods.
By creating an authentication sequence that includes both RADIUS and SAML server profiles, the firewall will attempt authentication with RADIUS first and, if that fails, will fall back to SAML. This enables both authentication types to function simultaneously during the transition period.
You can also configure an authentication profile that includes both the RADIUS Server Profile and the SAML Identity Provider server profile. This setup allows the firewall to use both RADIUS and SAML for authentication requests, and it will check both authentication methods in parallel.

NEW QUESTION # 62
.....

We update the NGFW-Engineer study materials frequently to let the client practice more and follow the change of development in the practice and theory. So that our worthy customers can always receive the most updated and the latest NGFW-Engineer learning guide. And according to our service, you can enjoy free updates for one year after you pay for the NGFW-Engineer Exam Questions. So if we update it, then we will auto send it to you. You won't miss any information that you need to pass the exam.

P.S. Free 2026 Palo Alto Networks NGFW-Engineer dumps are available on Google Drive shared by Exam4Tests: https://drive.google.com/open?id=19WEF0B7-RSWewAM126Jdj33gkjeK-ly9