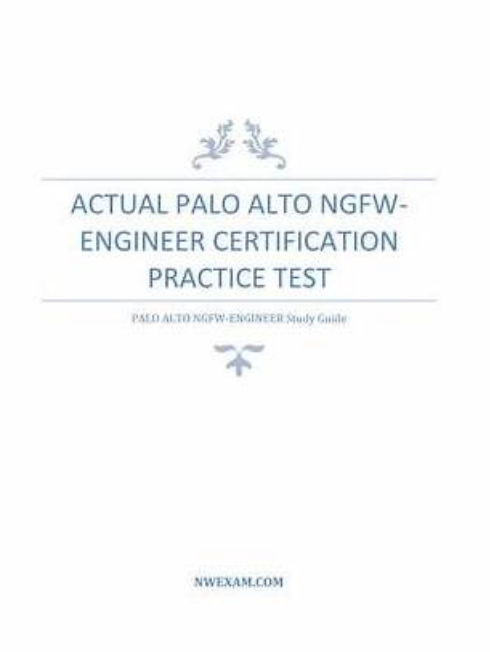
Valid Test NGFW-Engineer Bootcamp - NGFW-Engineer Valid Test Voucher



What's more, part of that ActualCollection NGFW-Engineer dumps now are free: https://drive.google.com/open?id=1ShsjKMGHusEER6vo_1poyZyFPzanusz_

The candidates can benefit themselves by using our NGFW-Engineer test engine and get a lot of test questions like exercises and answers. Our NGFW-Engineer exam questions will help them modify the entire syllabus in a short time. And the Software version of our NGFW-Engineer Study Materials have the advantage of simulating the real exam, so that the candidates have more experience of the practicing the real exam questions.

As a dumps provider, ActualCollection have a good reputation in the field. We are equipped with a team of IT elites who do much study in the Palo Alto Networks test questions and training materials. We check the updating of NGFW-Engineer Dumps PDF everyday to make sure you pass NGFW-Engineer valid test easily. The pass rate will be 100%.

>> Valid Test NGFW-Engineer Bootcamp <<

NGFW-Engineer Valid Test Voucher - Latest NGFW-Engineer Dumps Files

It would take a lot of serious effort to pass the Palo Alto Networks NGFW-Engineer exam, therefore it wouldn't be simple. So, you have to prepare yourself for this. But since we are here to assist you, you need not worry about how you will study for the Palo Alto Networks Next-Generation Firewall Engineer (NGFW-Engineer) exam dumps. You can get help from us on how to get ready for the Palo Alto Networks NGFW-Engineer Exam Questions. We will accomplish this objective by giving you access to some excellent NGFW-Engineer practice test material that will enable you to get ready for the Palo Alto Networks Next-Generation Firewall Engineer (NGFW-Engineer) exam dumps.

Palo Alto Networks NGFW-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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.
Topic 3	• 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.

Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q30-Q35):

NEW QUESTION # 30
What is the function of a Certificate Revocation List (CRL) in a PKI?

- A. Lists certificates pending renewal
- B. Lists expired certificates
- C. Lists certificates that have been revoked before their expiration date
- D. Lists all issued certificates

Answer: C

NEW QUESTION # 31
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. 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. Configure a single certificate profile for both user and machine certificates. Rely solely on CRLs for revocation to minimize complexity.

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 # 32
When deploying Palo Alto Networks NGFWs in a cloud service provider (CSP) environment, which method ensures high availability (HA) across multiple availability zones?

- A. Implementing Terraform templates for redundancy within one availability zone
- B. Using load balancer and health probes
- C. Deploying Ansible scripts for zone-specific scaling
- D. Configuring active/active HA

Answer: B

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 # 33
Which protocol and port number are used by default for IKE Phase 1 negotiations in an IPSec VPN?

- A. TCP 22
- B. UDP 4500
- C. UDP 500
- D. TCP 443

Answer: C

NEW QUESTION # 34
An NGFW engineer is establishing bidirectional connectivity between the accounting virtual system (VSYS) and the marketing VSYS. The traffic needs to transition between zones without leaving the firewall (no external physical connections). The interfaces for each VSYS are assigned to separate virtual routers (VRs), and inter-VR static routes have been configured. An external zone has been created correctly for each VSYS. Security policies have been added to permit the desired traffic between each zone and its respective external zone. However, the desired traffic is still unable to successfully pass from one VSYS to the other in either direction.
Which additional configuration task is required to resolve this issue?

- A. Create Security policies to allow the traffic between the two external zones.
- B. Add each VSYS to the list of visible virtual systems of the other VSYS.
- C. Create a transit VSYS and route all inter-VSYS traffic through it.
- D. Enable the "allow inter-VSYS traffic" option in both external zone configurations.

Answer: B

Explanation:
In Palo Alto Networks firewalls, each virtual system (VSYS) is typically isolated from other VSYSs, meaning that traffic between

different VSYSs cannot pass through the firewall by default. In this case, since the interfaces for each VSYS are assigned to separate virtual routers (VRs), and the desired traffic is still not passing between the two VSYSs, the firewall needs to be explicitly configured to allow traffic between them.
The required configuration is to add each VSYS to the list of visible virtual systems of the other VSYS. This allows inter-VSYS communication to be enabled, effectively permitting the traffic to pass between the zones of different VSYSs.

NEW QUESTION # 35
.....