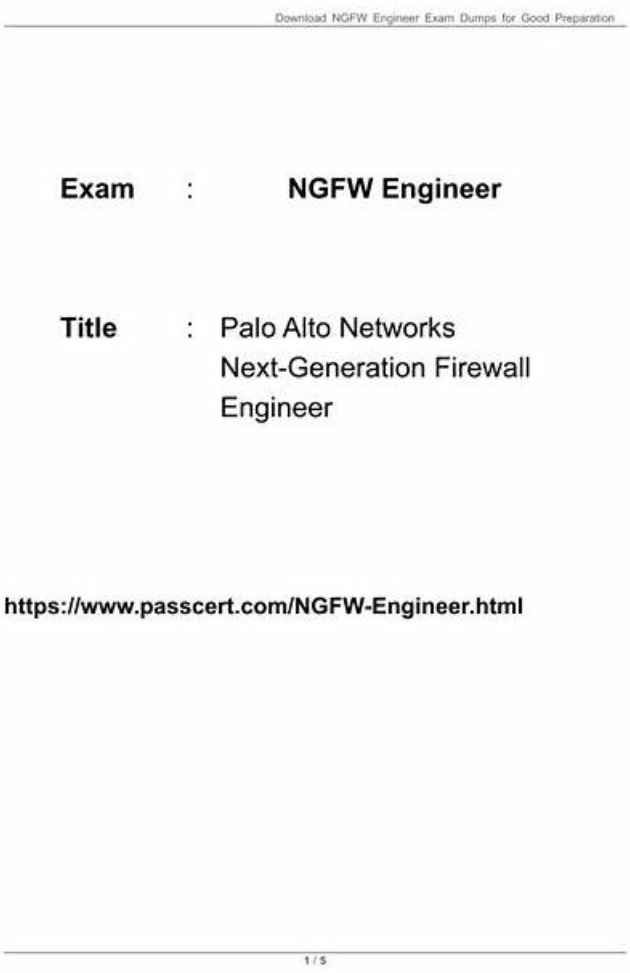
NGFW-Engineer Exam Score & NGFW-Engineer Valid Exam Notes



BTW, DOWNLOAD part of TroytecDumps NGFW-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1yUoEIW3PNhFe-hlN9itO5gwftYS7kUrz

You must be very surprised to see that our pass rate of the NGFW-Engineer study guide is high as 98% to 100%! We can tell you with data that this is completely true. The contents and design of NGFW-Engineer learning quiz are very scientific and have passed several official tests. Under the guidance of a professional team, you really find that NGFW-Engineer training engine is the most efficient product you have ever used.

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.

Excellent Palo Alto Networks NGFW-Engineer Exam Score Are Leading Materials & Effective NGFW-Engineer Valid Exam Notes

As is known to us, perfect after-sales service for buyers is a very high value. Our NGFW-Engineer Guide Torrent not only has the high quality and efficiency but also the perfect service system after sale. Our NGFW-Engineer exam questions can help you save much time, if you use our products, you just need to spend 20-30 hours on learning, and you will pass your exam successfully. What most important is that you can download our study materials about 5~10 minutes after you purchase.

Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q12-Q17):

NEW QUESTION # 12
Which CLI command is used to configure the management interface as a DHCP client?

- A. set network dhcp type management-interface
- B. set network dhcp interface management
- 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 # 13
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 only. Export daily policy configuration snapshots to Panorama for recordkeeping, but do not unify policy enforcement.
- B. Deploy a single CN-Series firewall in the on-premises data center to process traffic for all clusters, connecting remote clusters via VPN or peering. Manage this single instance through Panorama.
- C. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in each cluster, ensuring local insertion into the service mesh or CNI. Manage all CN-Series firewalls centrally from Panorama, applying uniform Security policies across on-

premises and cloud clusters.

- D. Configure the CN-Series only in public cloud clusters, and rely on Kubernetes Network Policies for on-premises cluster security. Synchronize partial policy information into Panorama manually as needed.

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 # 14
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 apply an authentication profile with the "SAML Identity Provider" Server Profile.
- B. Create an authentication sequence that includes both the "RADIUS" Server Profile and "SAML Identity Provider" Server Profile to run the two services in tandem.
- C. Create and add the "SAML Identity Provider" Server Profile to the authentication profile for the "RADIUS" Server Profile.
- D. Create a testing and rollback plan for the transition from Radius to SAML, as the two authentication profiles cannot be run in tandem.

Answer: B,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 # 15
When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

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

Answer: A

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 # 16

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. Configure each firewall independently to trust the root and intermediate CA certificates. 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.
- B. Distribute the root and intermediate CA certificates via Panorama as shared objects to ensure all firewalls have a consistent trust chain. Configure OCSP responder profiles on each firewall to offload revocation checks to an internal OCSP server while keeping CRL checks as a fallback. 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.
- C. Deploy self-signed certificates at each site to simplify local certificate validation and reduce dependencies on a centralized CA. 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.
- D. Obtain wildcard certificates from a public CA for both user and device authentication, and configure firewalls to perform CRL polling at the default update interval. 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 # 17
.....

□NGFW-Engineer Customizable Exam Mode

- New NGFW-Engineer Exam Notes □ Examcollection NGFW-Engineer Vce □ Advanced NGFW-Engineer Testing Engine □ Simply search for 《 NGFW-Engineer 》 for free download on ➤ www.pdfvce.com □ □Advanced NGFW-Engineer Testing Engine
- NGFW-Engineer practice materials - NGFW-Engineer guide torrent: Palo Alto Networks Next-Generation Firewall Engineer - NGFW-Engineer study guide □ Open { www.prep4pass.com } enter □ NGFW-Engineer □ and obtain a free download □NGFW-Engineer Valid Study Notes
- NGFW-Engineer Trustworthy Source □ Reliable NGFW-Engineer Test Guide □ NGFW-Engineer Practice Exam Online ➽ Go to website 「 www.pdfvce.com 」 open and search for ➤ NGFW-Engineer □ to download for free □ □NGFW-Engineer Customizable Exam Mode
- Web-Based Practice Tests: The Key to Palo Alto Networks NGFW-Engineer Exam Success □ Download ▹ NGFW-Engineer ◃ for free by simply searching on ✔ www.examsreviews.com □✔□ □NGFW-Engineer Valid Test Camp
- Updated Palo Alto Networks NGFW-Engineer Practice Questions in PDF Format □ Go to website □ www.pdfvce.com □ open and search for ➠ NGFW-Engineer □ to download for free □Pdf NGFW-Engineer Torrent
- Palo Alto Networks NGFW-Engineer questions and answers □ Search for ➠ NGFW-Engineer □ and download exam materials for free through □ www.prep4away.com □ □Advanced NGFW-Engineer Testing Engine
- playground.turing.aws.carboncode.co.uk, lms.ait.edu.za, daotao.wisebusiness.edu.vn, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, motionentrance.edu.np, techdrugsolution.com, dulanonline.com, lms.ait.edu.za, study.stcs.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2025 Palo Alto Networks NGFW-Engineer dumps are available on Google Drive shared by TroytecDumps: https://drive.google.com/open?id=1yUoEIW3PNhFe-hlN9itO5gwftYS7kUrz