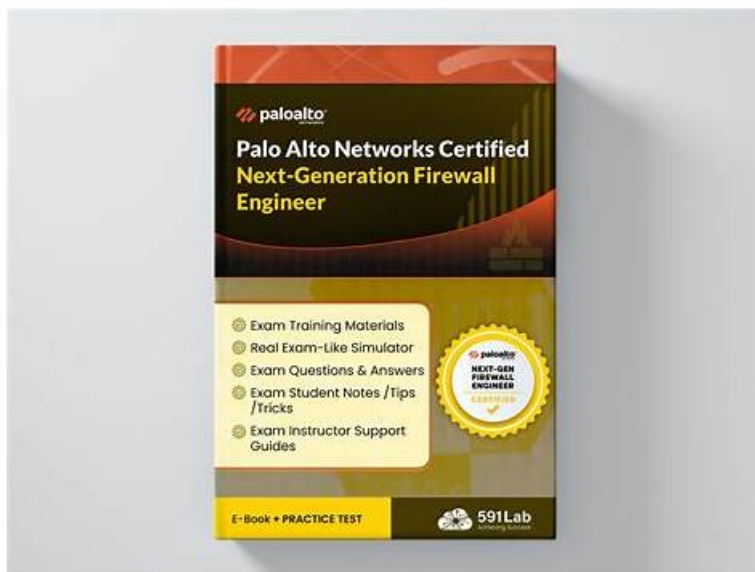


How Palo Alto Networks is so Confident in its Palo Alto Networks NGFW-Engineer Exam Questions?



BONUS!!! Download part of It-Tests NGFW-Engineer dumps for free: <https://drive.google.com/open?id=1LW48wsSw1c1SEzCaoTXjAtuaRgxMpq11>

It-Tests insists on providing you with the best and high quality exam dumps, aiming to ensure you 100% pass in the actual test. Being qualified with Palo Alto Networks certification will bring you benefits beyond your expectation. Our NGFW-Engineer practice training material will help you to enhance your specialized knowledge and pass your actual test with ease. NGFW-Engineer Questions are all checked and verified by our professional experts. Besides, the NGFW-Engineer answers are all accurate which ensure the high hit rate.

Palo Alto Networks NGFW-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> • 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 and 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 2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

Reliable NGFW-Engineer Dumps Free, NGFW-Engineer Exam Study Solutions

There are various individuals who have never shown up for the Palo Alto Networks Next-Generation Firewall Engineer certification test as of now. They know close to nothing about the Palo Alto Networks Next-Generation Firewall Engineer exam model and how to attempt the requests. Palo Alto Networks NGFW-Engineer Dumps give an unequivocal thought of the last preliminary of the year model and how a promising rookie ought to attempt the solicitation paper to score well.

Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q19-Q24):

NEW QUESTION # 19

To maintain security efficacy of its public cloud resources by using native tools, a company purchases Cloud NGFW credits to replicate the Panorama, PA-Series, and VM-Series devices used in physical data centers.

Resources exist on AWS and Azure:

The AWS deployment is architected with AWS Transit Gateway, to which all resources connect. The Azure deployment is architected with each application independently routing traffic. The engineer deploying Cloud NGFW in these two cloud environments must account for the following:

Minimize changes to the two cloud environments

Scale to the demands of the applications while using the least amount of compute resources. Allow the company to unify the Security policies across all protected areas. Which two implementations will meet these requirements? (Choose two.)

- A. Deploy Cloud NGFW for Azure in vNET/s, update the vNET/s routing to path traffic through the deployed NGFWs, and manage the policy with Panorama.
- B. Deploy Cloud NGFW for AWS in a centralized Security VPC, update the Transit Gateway to route all appropriate traffic through the Security VPC, and manage the policy with Panorama.
- C. Deploy Cloud NGFW for Azure in vWAN, create a vWAN to route all appropriate traffic to the Cloud NGFW attached to the vWAN, and manage the policy with local rules.
- D. Deploy a VM-Series firewall in AWS in each VPC, create an IPSec tunnel between AWS and Azure, and manage the policy with Panorama.

Answer: A,B

Explanation:

To meet the company's requirements - minimizing changes to the cloud environments, optimizing compute resources, and unifying security policies - the best approach is to deploy Cloud NGFW solutions natively for AWS and Azure while managing policies centrally with Panorama.

In Azure, using Cloud NGFW for Azure deployed within vNETs allows traffic to be routed through security appliances efficiently without requiring a complete re-architecture. This approach aligns with Azure's existing routing mechanism while maintaining security.

In AWS, deploying Cloud NGFW for AWS in a centralized Security VPC and integrating it with AWS Transit Gateway enables traffic inspection for all connected VPCs without modifying individual workloads.

This method ensures efficient scaling and minimal infrastructure changes while maintaining security consistency.

NEW QUESTION # 20

When creating a Log Forwarding profile on a PAN-OS firewall to direct logs to various external and internal systems, which set of methods is available?

- A. HTTP, RADIUS, SNMP
- B. Syslog, Panorama, SD-WAN
- C. Email, Syslog, NetFlow
- D. Panorama/Cloud logging, email, Syslog

Answer: D

Explanation:

Log Forwarding profiles in PAN-OS support forwarding logs to Panorama or cloud logging services, sending notifications via email,

and exporting logs to external systems using Syslog, which together form the supported log forwarding mechanisms for centralized management and integration.

NEW QUESTION # 21

A firewall administrator needs to configure a new Palo Alto Networks firewall so that its management interface automatically obtains an IP address, netmask, and default gateway from the network.

Which command should be executed in the CLI to accomplish this goal?

- A. `set deviceconfig system interface mgt mode dhcp`
- B. `configure system management-interface ip dynamic`
- C. `set network interface management dhcp enable`
- D. `set deviceconfig system type dhcp-client`

Answer: A

Explanation:

This command configures the management interface to operate in DHCP mode, allowing it to automatically obtain an IP address, subnet mask, and default gateway from the network's DHCP server.

NEW QUESTION # 22

A security administrator is creating a new custom report to get a consolidated view of network events and needs to select a database to query for the report data. Which valid set of databases is available for the task?

- A. Threat, URL Filtering, WildFire Submissions, GlobalProtect
- B. Data Filtering, IP-Tag, User-ID, Endpoint Security
- C. System, Config, Authentication, Session Flow
- D. Traffic, User-ID, Application Statistics, HIP Match

Answer: A

Explanation:

When generating custom reports on a Palo Alto Networks firewall, the administrator must first select the underlying database that the report will query. The firewall maintains two primary types of databases for reporting: Summary Databases and Detailed Logs. The Summary Databases aggregate data every 15 minutes for faster report generation, whereas Detailed Logs provide a granular look at every single event.

The valid databases available for custom reports include:

* Summary Databases: Traffic, Threat, URL Filtering, Application Statistics, and Tunnel Inspection.

* Detailed Logs: Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel, Authentication, and SCTP.

Option A is the correct answer because all four components (Threat, URL Filtering, WildFire Submissions, and GlobalProtect) are distinct, valid database types that can be selected from the "Database" dropdown menu in the Custom Report configuration (found under Monitor > Manage Custom Reports > Add).

Option B is also composed of valid databases; however, in the context of Palo Alto Networks certification objectives, Option A is typically the highlighted set for demonstrating visibility into security-related network events. Option C is incorrect because "Endpoint Security" is not a valid database name in the firewall's reporting engine (the firewall uses "HIP Match" for host information). Option D is incorrect because the "Config" and "System" logs are generally viewed through the standard Log Viewer and are not available as source databases for the Custom Report builder, nor is there a "Session Flow" database in this context.

NEW QUESTION # 23

A network administrator needs to replace the default self-signed certificate on a firewall with one signed by the company's internal certificate authority (CA).

Which two firewall features would require this new certificate to be assigned via an SSL/TLS service profile? (Choose two.)

- A. GlobalProtect gateway
- B. User-ID agent redistribution
- C. Authentication portal
- D. RADIUS server authentication

