Use Palo Alto Networks NetSec-Pro Exam Dumps And Get Successful

What's more, part of that ITexamReview NetSec-Pro dumps now are free: https://drive.google.com/open?id=1QbKES8n8G6d6ADEFBnwz93tTT05XZGDo

It is well known that certificates are not versatile, but without a Palo Alto Networks NetSec-Pro certification you are a little inferior to the same competitors in many ways. Compared with the people who have the same experience, you will have the different result and treatment if you have a Palo Alto Networks Network Security Professional NetSec-Pro Certification.

Palo Alto Networks NetSec-Pro Exam Syllabus Topics:

Topic	Details
Topic 1	• Platform Solutions, Services, and Tools: This section measures the expertise of security engineers and platform administrators in Palo Alto Networks NGFW and Prisma SASE products. It involves creating security and NAT policies, configuring Cloud-Delivered Security Services (CDSS) such as security profiles, User-ID and App-ID, decryption, and monitoring. It also covers the application of CDSS for IoT security, Enterprise Data Loss Prevention, SaaS Security, SD-WAN, GlobalProtect, Advanced WildFire, Threat Prevention, URL Filtering, and DNS security. Furthermore, it includes aligning AIOps with best practices through administration, dashboards, and Best Practice Assessments.
Topic 2	• Infrastructure Management and CDSS: This section tests the abilities of security operations specialists and infrastructure managers in maintaining and configuring Cloud-Delivered Security Services (CDSS) including security policies, profiles, and updates. It includes managing IoT security with device IDs and monitoring, as well as Enterprise Data Loss Prevention and SaaS Security focusing on data encryption, access control, and logging. It also covers maintenance and configuration of Strata Cloud Manager and Panorama for network security environments including supported products, device addition, reporting, and configuration management.

Topic 3	• Connectivity and Security: This part measures the skills of network engineers and security analysts in maintaining and configuring network security across on-premises, cloud, and hybrid environments. It covers network segmentation, security and network policies, monitoring, logging, and certificate management. It also includes maintaining connectivity and security for remote users through remote access solutions, network segmentation, security policy tuning, monitoring, logging, and certificate usage to ensure secure and reliable remote connections.
Topic 4	• Network Security Fundamentals: This section of the exam measures skills of network security engineers and covers key concepts such as application layer inspection for Strata and SASE products, differentiating between slow and fast path packet inspection, and the use of decryption methods including SSL Forward Proxy, SSL Inbound Inspection, SSH Proxy, and scenarios where no decryption is applied. It also includes applying network hardening techniques like Content-ID, Zero Trust principles, User-ID (including Cloud Identity Engine), Device-ID, and network zoning to enhance security on Strata and SASE platforms.

NetSec-Pro Reliable Exam Review - NetSec-Pro Test Dumps.zip

Since inception, our company has been working on the preparation of NetSec-Pro learning guide, and now has successfully helped tens of thousands of candidates around the world to pass the exam. As a member of the group who are about to take the NetSec-Pro Exam, are you worried about the difficulties in preparing for the exam? Maybe this problem can be solved today, if you are willing to spend a few minutes to try our NetSec-Pro actual exam.

Palo Alto Networks Network Security Professional Sample Questions (Q36-Q41):

NEW QUESTION # 36
Which zone is available for use in Prisma Access?

- A. Clientless VPN
- B. DMZ
- C. Intrazone
- D. Interzone

Answer: D

Explanation:
In Prisma Access, theinterzonesecurity policy rule isavailableand plays a crucial role in controlling traffic betweenzones.
"You can configure an interzone rule to control traffic that flows between different zones in Prisma Access, enabling granular security policy enforcement." (Source: Prisma Access Security Policies) This ensures comprehensive control of traffic crossing security boundaries in the cloud-delivered architecture.

NEW QUESTION # 37
What are two recommendations to ensure secure and efficient connectivity across multiple locations in a distributed enterprise network? (Choose two.)

- A. Implement a flat network design for simplified network management and reduced overhead.
- B. Create broad VPN policies for contractors working at branch locations.
- C. Employ centralized management and consistent policy enforcement across all locations.
- D. Use Prisma Access to provide secure remote access for branch users.

Answer: C,D

Explanation:
Prisma Access for secure remote access

"Prisma Access extends consistent security and optimized connectivity to branch locations, enabling secure access for mobile and branch users." (Source: Prisma Access Overview) Centralized management for consistent policy enforcement
"Centralized management using Strata Cloud Manager or Panorama ensures security policies and updates are uniformly applied across distributed locations, preventing policy drift and security gaps." (Source: Strata Cloud Manager Best Practices) These two practices are foundational for modern, distributed enterprise networks to maintain security posture and performance.

NEW QUESTION # 38
Which two tools can be used to configure Cloud NGFWs for AWS? (Choose two.)

- A. Cloud service provider's management console
- B. Panorama
- C. Cortex XSIAM
- D. Prisma Cloud management console

Answer: A,B

Explanation:
Cloud NGFW for AWS can be configured usingPanoramafor centralized management, as well as theAWS management consolefor native integration and configuration.
"You can configure Cloud NGFW for AWS using Panorama for centralized security management, or directly through the AWS management console to deploy and manage security services for your AWS resources." (Source: Cloud NGFW for AWS Guide)

NEW QUESTION # 39
Which two types of logs must be forwarded to Strata Logging Service for IoT Security to function?
(Choose two.)

- A. Enhanced application
- B. Threat
- C. URL Filtering
- D. WildFire

Answer: A,B

Explanation:
For IoT Security toaccurately classify and monitorIoT devices, the following logs must be forwarded to Strata Logging Service:
Enhanced application logs- provide detailed application usage and behaviors, essential for profiling device types and roles.
"Enhanced Application logs provide additional context on IoT device behavior and usage patterns, and must be forwarded to Strata Logging Service for IoT Security to build accurate Device-ID profiles." (Source: IoT Security Logging Requirements) Threat logs- essential for detecting suspicious or malicious activities by IoT devices.
"Threat logs are critical for identifying potential exploits or suspicious activities involving IoT devices and are required for accurate threat visibility within IoT Security." (Source: IoT Security Logs) These logs collectively ensure accurate device classification and real-time threat visibility.

NEW QUESTION # 40
Which two security services are required for configuration of NGFW Security policies to protect against malicious and misconfigured domains? (Choose two.)

- A. SaaS Security
- B. Advanced Threat Prevention
- C. Advanced WildFire
- D. Advanced DNS Security

Answer: B,D

Explanation:
Protecting againstmaliciousandmisconfigured domainsrequires two critical services:
Advanced Threat Prevention
Provides signature-based and advanced analysis to identify threats, including DNS-based attacks.

"Advanced Threat Prevention enables the NGFW to detect and prevent exploits and malware-based communications, including those leveraging DNS." (Source: Advanced Threat Prevention) Advanced DNS Security Specifically designed to detect and sinkhole malicious and misconfigured DNS queries.
"DNS Security uses real-time intelligence to block DNS-based threats, protect against data exfiltration, and automatically sinkhole suspicious domain lookups." (Source: DNS Security) Bycombiningthese services in security policies, NGFWs ensure robust protection against domain-based threats and misconfigurations.

NEW QUESTION # 41
......