

Valid Braindumps NetSec-Pro Files - NetSec-Pro Valid Exam Preparation



BONUS!!! Download part of Real4exams NetSec-Pro dumps for free: <https://drive.google.com/open?id=1WcwQNaWBUzRHjObPJSQzGKve8HLfSXi5>

A good brand is not a cheap product, but a brand that goes well beyond its users' expectations. The value of a brand is that the NetSec-Pro exam questions are more than just exam preparation tool -- it should be part of our lives, into our daily lives. Do this, therefore, our NetSec-Pro question guide has become the industry well-known brands, but even so, we have never stopped the pace of progress, we have been constantly updated the NetSec-Pro real study dumps. The most important thing is that the NetSec-Pro exam questions are continuously polished to be sold, so that users can enjoy the best service that our products bring. Our NetSec-Pro real study dumps provide users with comprehensive learning materials, so that users can keep abreast of the progress of The Times.

We have professional technicians to check the website every day, and you can have a clean and safe online shopping environment if you purchasing NetSec-Pro learning materials from us. In addition, we are pass guarantee and money back guarantee for NetSec-Pro exam dumps, and if you fail to pass the exam, we will give you full refund. We have free demo for you to have a try before buying NetSec-Pro Exam Materials of us, so that you can know what the complete version is like. We have online and offline service, and if you have any questions for NetSec-Pro exam dumps, you can consult us.

>> Valid Braindumps NetSec-Pro Files <<

NetSec-Pro Valid Exam Preparation - Dump NetSec-Pro Collection

The Palo Alto Networks Network Security Professional (NetSec-Pro) exam preparation material is available in three different formats for the customers. The formats are PDF format, web-based software, and Palo Alto Networks NetSec-Pro desktop practice exam software. The portable PDF format means customers can access real Palo Alto Networks Network Security Professional (NetSec-Pro) exam questions on their smartphones, tablets, and laptops. The PDF format can be printed and customers can also make proper NetSec-Pro exam notes.

Palo Alto Networks NetSec-Pro Exam Syllabus Topics:

Topic	Details

Topic 1	<ul style="list-style-type: none"> • 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.
Topic 2	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • 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.

Palo Alto Networks Network Security Professional Sample Questions (Q27-Q32):

NEW QUESTION # 27

Which set of practices should be implemented with Cloud Access Security Broker (CASB) to ensure robust data encryption and protect sensitive information in SaaS applications?

- A. Enable encryption for data-at-rest and in transit, regularly update encryption keys, and use strong encryption algorithms.
- B. Use default encryption keys provided by the SaaS provider.
- C. Do not enable encryption for data-at-rest to improve performance.
- D. Perform annual encryption key rotations.

Answer: A

Explanation:

CASB integration should focus on comprehensive data protection, which includes encryption for data-at-rest and in transit, frequent key updates, and using strong encryption algorithms to ensure confidentiality and data integrity.

"CASB solutions should enforce encryption for data-at-rest and in transit, implement key rotation policies, and leverage robust encryption algorithms to protect sensitive SaaS application data." (Source: CASB Deployment Best Practices)

NEW QUESTION # 28

A primary firewall in a high availability (HA) pair is experiencing a current failover issue with ICMP pings to a secondary device. Which metric should be reviewed for proper ICMP pings between the firewall pair?

- A. Link monitoring
- B. Heartbeat polling
- C. Non-functional state
- D. Bidirectional Forwarding Detection (BFD)

Answer: B

Explanation:

Heartbeat polling is a core HA function to monitor connectivity between HA peers, leveraging ICMP pings to determine link health and availability.

"Heartbeat Polling uses ICMP pings to verify the connectivity and health of the HA peers. If heartbeat polling fails, the firewall considers the peer to be down and may initiate failover." (Source: HA Link and Path Monitoring) If ICMP pings fail, checking heartbeat polling logs helps identify if link or path monitoring triggers the failover.

NEW QUESTION # 29

Which two prerequisites must be evaluated when decrypting internet-bound traffic? (Choose two.)

- A. SAML certificate
- B. Certificate pinning
- C. Incomplete certificate chains
- D. RADIUS profile

Answer: B,C

Explanation:

When implementing SSL Forward Proxy decryption for outbound traffic, two key challenges that must be evaluated are:

* Incomplete certificate chains: This occurs when the firewall cannot validate the entire certificate chain for a site, which may cause decryption failures.

* Certificate pinning: Applications like banking apps may use certificate pinning to prevent MITM (man-in-the-middle) attacks, and these applications will break if SSL Forward Proxy is used.

"When decrypting outbound SSL traffic, you must consider incomplete certificate chains, which can cause decryption to fail if the firewall cannot validate the entire chain. Also, be aware of certificate pinning in applications that prevents decryption by rejecting forged certificates." (Source: Palo Alto Networks Decryption Concepts)

NEW QUESTION # 30

How can a firewall administrator block a list of 300 unique URLs in the most time-efficient manner?

- A. Block multiple predefined URL categories.
- B. Use application filters to block the App-IDs.
- C. Use application groups to block the App-IDs.
- D. Import the list into a custom URL category.

Answer: D

Explanation:

For large lists of specific URLs, creating a custom URL category and importing the list is the most efficient approach for granular URL filtering.

"You can create custom URL categories to define specific URLs or patterns and enforce policies for these categories. This is the most efficient way to handle large sets of URLs." (Source: Custom URL Categories) This approach saves time compared to manual rule creation or using generic application filters.

NEW QUESTION # 31

What key capability distinguishes Content-ID technology from conventional network security approaches?

- A. It relies primarily on reputation-based filtering.
- B. It exclusively monitors network traffic volumes.
- C. It provides single-pass application layer inspection for real-time threat prevention.
- D. It performs packet header analysis short of deep packet inspection.

Answer: C

Explanation:

Content-ID is the core of Palo Alto Networks' prevention architecture, providing single-pass application layer inspection to deliver real-time threat prevention across all traffic.

"Content-ID uses a single-pass architecture to perform application-layer (Layer 7) traffic inspection and real-time threat prevention. Unlike traditional firewalls that rely on multiple scans, Content-ID inspects traffic once to enforce multiple security controls simultaneously." (Source: Content-ID Overview) By consolidating security functions in a single pass, it ensures both efficiency and comprehensive security.

