

最新的NetSec-Pro認證考試資料匯總



人生舞臺的大幕隨時都可能拉開，關鍵是你願意表演，還是選擇躲避，能把在面前行走的機會抓住的人，十有八九都是成功的。所以你必須抓住Fast2test這個機會，讓你隨時可以展現你的技能，Fast2test Palo Alto Networks的NetSec-Pro考試培訓資料就是你通過認證的最有效的方法，有了這個認證，你將在你人生的藍圖上隨意揮灑，實現你的夢想，走向成功。要做就做一個勇往直前的人，那樣的人生才有意義。

Fast2test剛剛發布了最新的NetSec-Pro認證考試所有更新的問題及答案，來確保您考試成功通過。我們提供最新的PDF和軟件版本的問題和答案，可以保證考生的NetSec-Pro考試100%通過。在我們的網站上，您將獲得我們提供的Palo Alto Networks NetSec-Pro免費的PDF版本的DEMO試用，您會發現這絕對是最值得信賴的學習資料。對於擁有高命中率的Palo Alto Networks NetSec-Pro考古題，還在等什么，趕快下載最新的題庫資料來準備考試吧！

>> NetSec-Pro考試 <<

最真實的NetSec-Pro認證考試的題目與答案

我們Fast2test的 Palo Alto Networks的NetSec-Pro的考題資料是按照相同的教學大綱來來研究的，同時也不斷升級我們的培訓材料，所以我們的考試培訓資料包括試題及答案，和實際的考試相似度非常高，所以形成了我們Fast2test的通過率也是非常的高，這也是不可否認的事實，由此知道Fast2test Palo Alto Networks的NetSec-Pro考試培訓資料對考生的幫助，而且我們的價格絕對合理，適合每位IT認證的考生。

Palo Alto Networks NetSec-Pro 考試大綱：

主題	簡介
主題 1	<ul style="list-style-type: none">• NGFW and SASE Solution Functionality: This part assesses the knowledge of firewall administrators and network architects on the functions of various Palo Alto Networks firewalls including Cloud NGFWs, PA-Series, CN-Series, and VM-Series. It covers perimeter and core security, zone security and segmentation, high availability, security and NAT policy implementation, as well as monitoring and logging. Additionally, it includes the functionality of Prisma SD-WAN with WAN optimization, path and NAT policies, zone-based firewall, and monitoring, plus Prisma Access features such as remote user and network configuration, application access, policy enforcement, and logging. It also evaluates options for managing Strata and SASE solutions through Panorama and Strata Cloud Manager.

主題 2	<ul style="list-style-type: none"> • 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.
主題 3	<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.
主題 4	<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.

最新的 Network Security Administrator NetSec-Pro 免費考試真題 (Q12-Q17):

問題 #12

A network administrator obtains Palo Alto Networks Advanced Threat Prevention and Advanced DNS Security subscriptions for edge NGFWs and is setting up security profiles. Which step should be included in the initial configuration of the Advanced DNS Security service?

- A. Create overrides for all company owned FQDNs.
- B. Create a decryption policy rule to decrypt DNS-over-TLS / port 853 traffic.
- **C. Configure DNS Security signature policy settings to sinkhole malicious DNS queries.**
- D. Enable Advanced Threat Prevention with default settings and only focus on high-risk traffic.

答案: C

解題說明:

Advanced DNS Security uses a signature policy to sinkhole malicious DNS queries and prevent them from resolving.

"The DNS Security service integrates with Anti-Spyware profiles, and you must configure signature policy settings to sinkhole malicious queries. This proactively stops traffic to known malicious domains." (Source: Configure DNS Security) Sinkholing ensures that DNS queries to malicious FQDNs are redirected to a safe IP, preventing compromise.

問題 #13

When configuring Security policies on VM-Series firewalls, which set of actions will ensure the most comprehensive Security policy enforcement?

- **A. Configure policies using User-ID and App-ID, enable decryption, apply appropriate security profiles to rules, and update regularly with dynamic updates.**
- B. Configure port-based policies, check threat logs weekly, conduct software updates annually, and enable decryption.
- C. Configure a block policy for all malicious inbound traffic, configure an allow policy for all outbound traffic, and update regularly with dynamic updates.
- D. Configure all default policies provided by the firewall, use Policy Optimizer, and adjust security rules after an incident occurs.

答案: A

解題說明:

A comprehensive security approach uses:

- * User-ID for identity-based policies
- * App-ID for application-based security
- * Decryption to inspect encrypted traffic
- * Security profiles to enforce protections
- * Dynamic updates to ensure up-to-date threat coverage

"For comprehensive security, combine User-ID, App-ID, decryption, and security profiles. Keep the firewall updated with dynamic content updates to maintain the strongest security posture." (Source: Best Practices for Security Policy) This ensures real-time, identity-aware, and application-centric security enforcement.

問題 #14

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

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

答案: **D**

解題說明:

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.

問題 #15

Which functionality does an NGFW use to determine whether new session setups are legitimate or illegitimate?

- A. SYN bit
- **B. SYN cookies**
- C. SYN flood protection
- D. Random Early Detection (RED)

答案: **B**

解題說明:

To prevent SYN flood attacks, the NGFW uses SYN cookies to validate legitimate session establishment.

"SYN cookies allow the firewall to verify the legitimacy of new session requests without allocating resources until the handshake is completed. This prevents SYN flood attacks from exhausting system resources." (Source: Flood Protection Best Practices) SYN cookies mitigate resource exhaustion by ensuring only legitimate connections are established.

問題 #16

Using Prisma Access, which solution provides the most security coverage of network protocols for the mobile workforce?

- A. Explicit proxy
- B. Enterprise browser
- **C. Client-based VPN**
- D. Clientless VPN

答案: **C**

解題說明:

Client-based VPN solutions like GlobalProtect provide full coverage for the mobile workforce by extending the enterprise security stack to remote endpoints. It establishes a secure tunnel, allowing consistent security policies across the enterprise perimeter and the mobile workforce.

