

Latest Exam Questions PCCP Vce Offer You The Best Valid Exam Book | Palo Alto Networks Certified Cybersecurity Practitioner



DOWNLOAD the newest Prep4King PCCP PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1e7VNFuEfDbtHFT9kFgsjZUYNp2CxJ4W>

This kind of polished approach is beneficial for a commendable grade in the Palo Alto Networks Certified Cybersecurity Practitioner (PCCP) exam. While attempting the exam, take heed of the clock ticking, so that you manage the Palo Alto Networks PCCP questions in a time-efficient way. Even if you are completely sure of the correct answer to a question, first eliminate the incorrect ones, so that you may prevent blunders due to human error.

If candidates want to obtain certifications candidates should notice studying methods. If you do not want to purchase our Palo Alto Networks PCCP new exam bootcamp materials and just want to study yourself, willpower is the most important. Passing so many exams is really not easy. Reasonable studying methods and relative work experience make you half the work with double the results. PCCP New Exam Bootcamp materials will be a shortcut for you.

>> [Exam Questions PCCP Vce](#) <<

Palo Alto Networks PCCP Valid Exam Book & New PCCP Dumps Book

The PCCP guide dump from our company is compiled by a lot of excellent experts and professors in the field. In order to help all customers pass the exam in a short time, these excellent experts and professors tried their best to design the study version, which is very convenient for a lot of people who are preparing for the PCCP exam. You can find all the study materials about the exam by the study version from our company. More importantly, we can assure you that if you use our PCCP Certification guide, you will never miss any important and newest information. We will send you an email about the important study information every day in order to help you study well. We believe that our PCCP exam files will be most convenient for all people who want to take an exam.

Palo Alto Networks PCCP Exam Syllabus Topics:

Topic	Details
-------	---------

Topic 1	<ul style="list-style-type: none"> Secure Access: This part of the exam measures skills of a Secure Access Engineer and focuses on defining and differentiating Secure Access Service Edge (SASE) and Secure Service Edge (SSE). It covers challenges related to confidentiality, integrity, and availability of data and applications across data, private apps, SaaS, and AI tools. It examines security technologies including secure web gateways, enterprise browsers, remote browser isolation, data loss prevention (DLP), and cloud access security brokers (CASB). The section also describes Software-Defined Wide Area Network (SD-WAN) and Prisma SASE solutions such as Prisma Access, SD-WAN, AI Access, and enterprise DLP.
Topic 2	<ul style="list-style-type: none"> Cloud Security: This section targets a Cloud Security Specialist and addresses major cloud architectures and topologies. It discusses security challenges like application security, cloud posture, and runtime security. Candidates will learn about technologies securing cloud environments such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), as well as the functions of a Cloud Native Application Protection Platform (CNAPP) and features of Cortex Cloud.
Topic 3	<ul style="list-style-type: none"> Endpoint Security: This domain is aimed at an Endpoint Security Analyst and covers identifying indicators of compromise (IOCs) and understanding the limits of signature-based anti-malware. It includes concepts like User and Entity Behavior Analytics (UEBA), endpoint detection and response (EDR), and extended detection and response (XDR). It also describes behavioral threat prevention and endpoint security technologies such as host-based firewalls, intrusion prevention systems, device control, application control, disk encryption, patch management, and features of Cortex XDR.
Topic 4	<ul style="list-style-type: none"> Cybersecurity: This section of the exam measures skills of a Cybersecurity Practitioner and covers fundamental concepts of cybersecurity, including the components of the authentication, authorization, and accounting (AAA) framework, attacker techniques as defined by the MITRE ATT&CK framework, and key principles of Zero Trust such as continuous monitoring and least privilege access. It also addresses understanding advanced persistent threats (APT) and common security technologies like identity and access management (IAM), multi-factor authentication (MFA), mobile device and application management, and email security.
Topic 5	<ul style="list-style-type: none"> Network Security: This domain targets a Network Security Specialist and includes knowledge of Zero Trust Network Access (ZTNA) characteristics, functions of stateless and next-generation firewalls (NGFWs), and the purpose of microsegmentation. It also covers common network security technologies such as intrusion prevention systems (IPS), URL filtering, DNS security, VPNs, and SSL TLS decryption. Candidates must understand the limitations of signature-based protection, deployment options for NGFWs, cybersecurity concerns in operational technology (OT) and IoT, cloud-delivered security services, and AI-powered security functions like Precision AI.

Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q78-Q83):

NEW QUESTION # 78

Which of the following is an AWS serverless service?

- A. Lambda
- B. Beta
- C. Delta
- D. Kappa

Answer: A

Explanation:

Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

NEW QUESTION # 79

A doctor receives an email about her upcoming holiday in France. When she clicks the URL website link in the email, the connection is blocked by her office firewall because it's a known malware website. Which type of attack includes a link to a malware website in an email?

- A. **phishing**
- B. spam
- C. whaling
- D. pharming

Answer: A

Explanation:

Phishing is a type of attack that involves sending fraudulent emails that appear to be from legitimate sources, such as banks, companies, or individuals, in order to trick recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information¹². The link to a malware website in the email is an example of a malicious link, which may lead to the installation of malware, ransomware, spyware, or other malicious software on the user's device, or the redirection to a fake website that mimics a legitimate one, where the user may be asked to enter their credentials, personal information, or financial details³⁴. Phishing emails often use social engineering techniques, such as creating a sense of urgency, curiosity, or fear, to persuade the user to click on the link or attachment, or to reply to the email⁵. Phishing emails may also spoof the sender's address, domain, or logo, to make them look more authentic and trustworthy⁶.

Whaling, pharming, and spam are not the correct answers for this question. Whaling is a specific type of phishing that targets high-profile individuals, such as executives, celebrities, or politicians, with the aim of stealing their confidential information or influencing their decisions⁷. Pharming is a type of attack that involves redirecting the user's web browser to a fake website, even if they enter the correct URL, by modifying the DNS server or the user's hosts file. Spam is the unsolicited or unwanted electronic messages, such as emails, texts, or instant messages, that are sent in bulk to a large number of recipients, usually for advertising, marketing, or scamming purposes. References:

- * [What is phishing? | Malwarebytes](#)
- * [Phishing - Wikipedia](#)
- * [Don't Panic! Here's What To Do If You Clicked On A Phishing Link](#)
- * [How can Malware spread through Email and How to Protect](#)
- * [What is phishing? How this cyber attack works and how to prevent it ...](#)
- * [Identifying Illegitimate Email Links | Division of Information Technology](#)
- * [What is whaling? | NortonLifeLock](#)
- * [\[What is pharming? | NortonLifeLock\]](#)
- * [\[What is spam? | NortonLifeLock\]](#)

NEW QUESTION # 80

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. **Credit card number**
- B. A symmetric encryption key
- C. National security information
- D. Trade secret

Answer: A

Explanation:

A credit card number is an example of PII that you need to prevent from leaving your enterprise network. PII, or personally identifiable information, is any information that can be used to identify an individual, either alone or in combination with other data. PII can be sensitive or non-sensitive, depending on the level of protection required and the potential harm if exposed. Sensitive PII includes data that can directly identify an individual and cause significant harm if leaked or stolen, such as financial information, medical records, or government-issued ID numbers. Non-sensitive PII includes data that is easily accessible from public sources and does not pose a high risk of identity theft, such as zip code, race, or gender. A credit card number is a sensitive PII because it can be used to access the cardholder's account, make fraudulent transactions, or steal their identity. Therefore, it is important to prevent credit card numbers from leaving the enterprise network, where they could be intercepted by hackers, malicious insiders, or third parties. To protect credit card numbers and other sensitive PII, enterprises should implement data security measures such as encryption, tokenization, masking, access control, auditing, and monitoring. Additionally, enterprises should comply with data privacy laws and standards that regulate the collection, use, and protection of PII, such as the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), or the California Consumer Privacy Act (CCPA).

References:

- * What is PII? Examples, laws, and standards | CSO Online
- * What is Personally Identifiable Information (PII)? | IBM
- * What Is Personally Identifiable Information (PII)? Types and Examples
- * What is PII (personally identifiable information)? - Cloudflare
- * What is Personally Identifiable Information (PII)? - Data Privacy Manager

NEW QUESTION # 81

Identify a weakness of a perimeter-based network security strategy to protect an organization's endpoint systems.

- A. It cannot identify command-and-control traffic
- **B. It assumes that every internal endpoint can be trusted**
- C. It cannot monitor all potential network ports
- D. It assumes that all internal devices are untrusted

Answer: B

Explanation:

A perimeter-based network security strategy relies on firewalls, routers, and other devices to create a boundary between the internal network and the external network. This strategy assumes that every internal endpoint can be trusted, and that any threat comes from outside the network. However, this assumption is flawed, as internal endpoints can also be compromised by malware, phishing, insider attacks, or other methods. Once an attacker gains access to an internal endpoint, they can use it to move laterally within the network, bypassing the perimeter defenses. Therefore, a perimeter-based network security strategy is not sufficient to protect an organization's endpoint systems, and a more comprehensive approach, such as Zero Trust, is needed. References:

- * Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCT)
- * Traditional perimeter-based network defense is obsolete-transform to a Zero Trust model
- * What is Network Perimeter Security? Definition and Components | Acalvio

NEW QUESTION # 82

What are two examples of an attacker using social engineering? (Choose two.)

- **A. Acting as a company representative and asking for personal information not relevant to the reason for their call**
- **B. Convincing an employee that they are also an employee**
- C. Leveraging open-source intelligence to gather information about a high-level executive
- D. Compromising a website and configuring it to automatically install malicious files onto systems that visit the page

Answer: A,B

Explanation:

Social engineering attacks manipulate human trust to gain unauthorized access or information. Convincing an employee that an attacker is also an employee builds rapport, lowering defenses for information disclosure or credential sharing. Similarly, impersonating a company representative and requesting unrelated personal data exploits authority bias to deceive victims. These tactics exploit psychological vulnerabilities rather than technical flaws and are prevalent initial steps in multi-stage attacks. Palo Alto Networks highlights the importance of training, multi-factor authentication, and behavior-based threat detection to mitigate social engineering risks effectively.

NEW QUESTION # 83

.....

On a regular basis, we update the PDF version to improve the PCCP Questions and accurately reflect any changes that have been made to the test content. We know that Palo Alto Networks Certified Cybersecurity Practitioner (PCCP) certification exam costs can be high, with registration fees often running between \$100 and \$1000. We provide a free demo version of our product to ensure you are completely satisfied with our Palo Alto Networks Certification Exams preparation material. The purpose of this free demo is to help you make a well-informed decision.

PCCP Valid Exam Book: <https://www.prep4king.com/PCCP-exam-prep-material.html>

- Hot Exam Questions PCCP Vce Free PDF | Latest PCCP Valid Exam Book: Palo Alto Networks Certified Cybersecurity Practitioner Copy URL www.prepawaypdf.com open and search for PCCP to download for free

Training PCCP Kit

BONUS!!! Download part of Prep4King PCCP dumps for free: <https://drive.google.com/open?id=1e7VNxFuEfDbtHFT9kFgrsjZUYNp2CxJ4W>