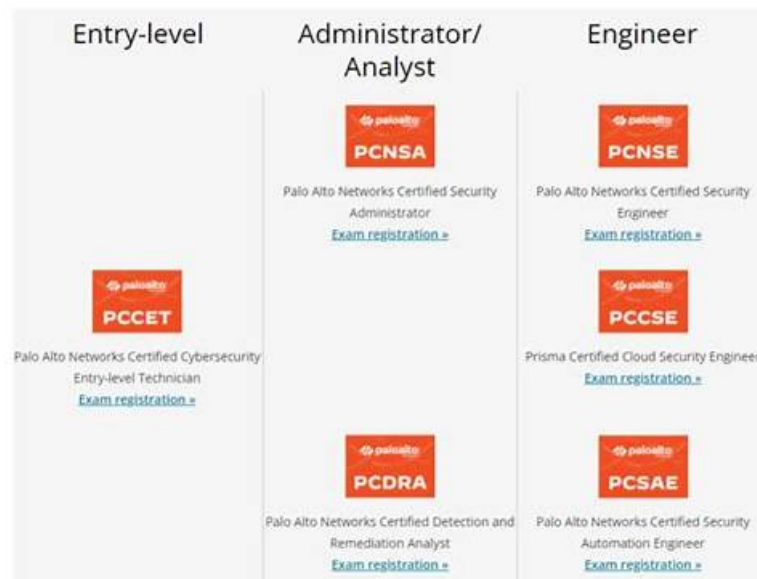


Go With Palo Alto Networks PCCP Exam Questions For 100% Success



BTW, DOWNLOAD part of PracticeDump PCCP dumps from Cloud Storage: <https://drive.google.com/open?id=1Y005WpYNy2EJW2McESRIZWLvjai7yV3t>

It is acknowledged that there are numerous PCCP learning questions for candidates for the exam, however, it is impossible for you to summarize all of the key points in so many materials by yourself. But since you have clicked into this website for PCCP practice materials you need not to worry about that at all because our company is especially here for you to solve this problem. We have a lot of regular customers for a long-term cooperation now since they have understood how useful and effective our PCCP Actual Exam is. So will you!

Profit from the opportunity to get these top-notch exam questions for the Palo Alto Networks PCCP certification test. We guarantee you that our top-rated Palo Alto Networks PCCP practice exam (PDF, desktop practice test software, and web-based practice exam) will enable you to pass the Palo Alto Networks PCCP Certification Exam on the very first go.

>> Valid PCCP Exam Syllabus <<

Best Way to Prepare For Palo Alto Networks PCCP Certification Exam

God wants me to be a person who have strength, rather than a good-looking doll. When I chose the IT industry I have proven to God my strength. But God forced me to keep moving. Palo Alto Networks PCCP exam is a major challenge in my life, so I am desperately trying to learn. But it does not matter, because I purchased PracticeDump's Palo Alto Networks PCCP Exam Training materials. With it, I can pass the Palo Alto Networks PCCP exam easily. Road is under our feet, only you can decide its direction. To choose PracticeDump's Palo Alto Networks PCCP exam training materials, and it is equivalent to have a better future.

Palo Alto Networks PCCP Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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 3	<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 4	<ul style="list-style-type: none"> Security Operations: This final section measures skills of a Security Operations Analyst and covers key characteristics and practices of threat hunting and incident response processes. It explains functions and benefits of security information and event management (SIEM) platforms, security orchestration, automation, and response (SOAR) tools, and attack surface management (ASM) platforms. It also highlights the functionalities of Cortex solutions, including XSOAR, Xparse, and XSIAM, and describes services offered by Palo Alto Networks' Unit 42.

Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q59-Q64):

NEW QUESTION # 59

What should a security operations engineer do if they are presented with an encoded string during an incident investigation?

- A. Append it to the investigation notes but do not alter it.
- B. Save it to a new file and run it in a sandbox.
- C. Run it against VirusTotal.
- D. Decode the string and continue the investigation.

Answer: D

Explanation:

An encoded string is a common technique used by attackers to obfuscate their malicious code or data. By decoding the string, a security operations engineer can reveal the true nature and intent of the attacker, and potentially discover indicators of compromise (IOCs) such as IP addresses, domain names, file names, etc.

Decoding the string can also help the engineer to determine the type and severity of the incident, and the appropriate response actions. Therefore, decoding the string and continuing the investigation is the best option among the given choices. Saving the string to a new file and running it in a sandbox may be risky, as it could execute the malicious code and cause further damage. Running the string against VirusTotal may not yield any useful results, as the string may not be recognized by any antivirus engines. Appending the string to the investigation notes but not altering it may not provide any additional insight into the incident, and may delay the response process. References:

- * 1: SANS Digital Forensics and Incident Response Blog | Strings, Strings, Are Wonderful Things
- * 2: 5 Minute Forensics: Decoding PowerShell Payloads - Tevora
- * 3: Known plaintext analysis of encoded strings - SANS Institute
- * 4: Palo Alto Networks Certified Cybersecurity Entry-level Technician - Palo Alto Networks
- * 5: 10 Palo Alto Networks PCCET Exam Practice Questions - CBT Nuggets

NEW QUESTION # 60

Which of these ports is normally associated with HTTPS?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:

HTTPS is a protocol that encrypts and secures the communication between web browsers and servers. HTTPS uses SSL or TLS certificates to establish a secure connection and prevent unauthorized access or tampering of data. HTTPS typically uses port 443, which is the default port for HTTPS connections. Port 443 is different from port 80, which is the default port for HTTP connections. HTTP is an unencrypted and insecure protocol that can expose sensitive information or allow malicious attacks. Port 443 is also different from port 5050, which is a common port for some applications or services, such as Yahoo Messenger or SIP. Port 5050 is not associated with HTTPS and does not provide any encryption or security. Port 443 is also different from port 25, which is the default port for SMTP, the protocol used for sending and receiving emails. Port 25 is not associated with HTTPS and does not encrypt the email content or headers. References:

*Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Palo Alto Networks

*HTTPS Protocol: What is the Default Port for SSL & Common TCP Ports

*What is HTTPS? | Cloudflare

*Can I use another port other than 443 for HTTPS/SSL communication?

NEW QUESTION # 61

From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

- A. Unit 52
- B. MineMeld
- C. BrightCloud
- **D. PAN-DB**

Answer: D

Explanation:

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

NEW QUESTION # 62

Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

- A. User and Entity Behavior Analytics (UEBA)
- B. User-ID
- **C. Identity and Access Management (IAM)**
- D. Lightweight Directory Access Protocol (LDAP)

Answer: C

Explanation:

Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

NEW QUESTION # 63

Which of the following is a Routed Protocol?

- A. Transmission Control Protocol (TCP)
- B. Routing Information Protocol (RIP)
- **C. Internet Protocol (IP)**
- D. Domain Name Service (DNS)

Answer: C

Explanation:

A routed protocol is a protocol by which data can be routed. It provides appropriate addressing information in its internet layer or

Examples of routed protocols are the Internet Protocol (IP) and Internetwork Packet Exchange (IPX). IP is the most widely used routed protocol on the Internet and other networks. It assigns a unique logical address to each device and enables data to be fragmented, reassembled, and routed across multiple networks. References:

- • • • •

P.S. Free & New PCCP dumps are available on Google Drive shared by PracticeDump: <https://drive.google.com/open?id=1Y005WpYNy2EJW2McESRIZWLvja17yV3t>