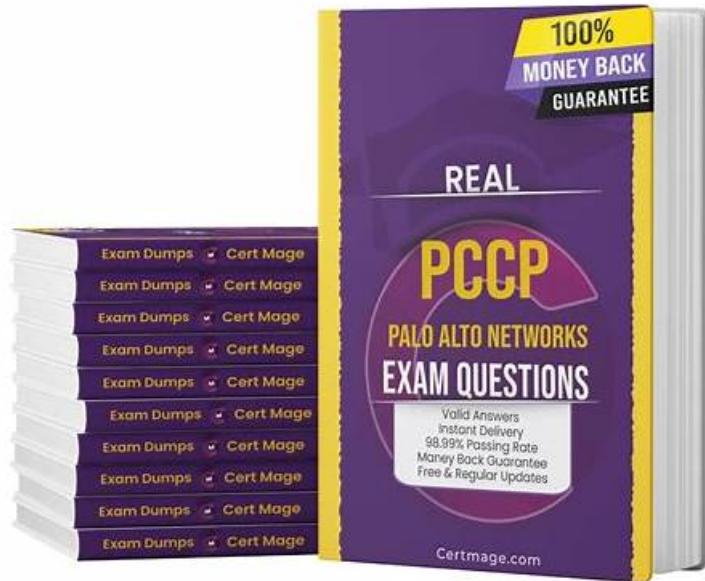


Palo Alto Networks PCCP Download Free Dumps, New PCCP Test Syllabus



What's more, part of that ExamDumpsVCE PCCP dumps now are free: <https://drive.google.com/open?id=1twYPvT3O7Fam1-n2xsDhwunQ0Po03Ld>

One more thing to give you an idea about the top features of Palo Alto Networks Certified Cybersecurity Practitioner (PCCP) exam questions before purchasing, the ExamDumpsVCE are offering free ExamDumpsVCE PCCP Exam Questions demo download facility. This facility is being offered in all three ExamDumpsVCE PCCP exam practice question formats.

Palo Alto Networks PCCP Exam Syllabus Topics:

Topic	Details
Topic 1	<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, Xpanse, and XSIAM, and describes services offered by Palo Alto Networks' Unit 42.
Topic 2	<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 3	<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 4	<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 5	<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.

>> Palo Alto Networks PCCP Download Free Dumps <<

Quiz Palo Alto Networks - PCCP - Palo Alto Networks Certified Cybersecurity Practitioner Authoritative Download Free Dumps

With the help of the Palo Alto Networks PCCP brain dumps and preparation material provided by ExamDumpsVCE, you will be able to get PCCP certified at the first attempt. Our experts have curated an amazing PCCP exam guide for passing the PCCP exam. You can get the desired outcome by preparing yourself from the PCCP Exam Dumps material provided by ExamDumpsVCE. We frequently update our PCCP exam preparation material to reflect the latest changes in the PCCP exam syllabus.

Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q79-Q84):

NEW QUESTION # 79

Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

- A. endpoint NIC ACLs
- B. strong endpoint passwords
- C. endpoint disk encryption
- D. **endpoint antivirus software**

Answer: D

Explanation:

Endpoint antivirus software is a type of software designed to help detect, prevent, and eliminate malware on devices, such as laptops, desktops, smartphones, and tablets. Endpoint antivirus software can block viruses that are not seen and blocked by the perimeter firewall, which is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. Perimeter firewall can block some known viruses, but it may not be able to detect and stop new or unknown viruses that use advanced techniques to evade detection. Endpoint antivirus software can provide an additional layer of protection by scanning the files and processes on the devices and using various methods, such as signatures, heuristics, behavior analysis, and cloud-based analysis, to identify and remove malicious code123. References:

* What Is Endpoint Antivirus? Key Features & Solutions Explained - Trellix

* Microsoft Defender for Endpoint | Microsoft Security

* Download ESET Endpoint Antivirus | ESET

NEW QUESTION # 80

Which scenario highlights how a malicious Portable Executable (PE) file is leveraged as an attack?

- A. Embedding the file inside a pdf to be downloaded and installed
- B. Laterally transferring the file through a network after being granted access
- C. Setting up a web page for harvesting user credentials
- D. Corruption of security device memory spaces while file is in transit

Answer: A

Explanation:

Malicious Portable Executable (PE) files hidden inside PDFs represent a stealthy delivery tactic where attackers embed executable payloads within seemingly benign documents. When a user opens the PDF, the embedded PE executes, potentially installing malware. This approach combines social engineering with file obfuscation to bypass traditional detection methods. Palo Alto Networks' Advanced WildFire sandboxing inspects such files by detonating them in isolated environments to observe behavior and identify hidden threats. This detection technique is critical for uncovering evasive malware concealed within common file types before they reach end-users.

NEW QUESTION # 81

Which security component can detect command-and-control traffic sent from multiple endpoints within a corporate data center?

- A. Next-generation firewall
- B. Port-based firewall
- C. Personal endpoint firewall
- D. Stateless firewall

Answer: A

Explanation:

A next-generation firewall (NGFW) is a security component that can detect command-and-control (C2) traffic sent from multiple endpoints within a corporate data center. A NGFW is a network device that combines traditional firewall capabilities with advanced features such as application awareness, intrusion prevention, threat intelligence, and cloud-based analysis. A NGFW can identify and block C2 traffic by inspecting the application layer protocols, signatures, and behaviors of the network traffic, as well as correlating the traffic with external sources of threat intelligence. A NGFW can also leverage inline cloud analysis to detect and prevent zero-day C2 threats in real-time. A NGFW can provide granular visibility and control over the network traffic, as well as generate alerts and reports on the C2 activity. References:

- * Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
- * Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK
- * Advanced Threat Prevention: Inline Cloud Analysis - Palo Alto Networks

NEW QUESTION # 82

TCP is the protocol of which layer of the OSI model?

- A. Application
- B. Data Link
- C. Session
- D. Transport

Answer: D

Explanation:

TCP stands for Transmission Control Protocol, and it is one of the main protocols used in the internet. TCP provides reliable, ordered, and error-free delivery of data between applications 1. In terms of the OSI model, TCP is a transport-layer protocol. The transport layer is the fourth layer of the OSI model, and it is responsible for establishing end-to-end connections, segmenting data into packets, and ensuring reliable and efficient data transfer 2. The transport layer also provides flow control, congestion control, and error detection and correction mechanisms 2. TCP is not the only transport-layer protocol; another common one is UDP (User Datagram Protocol), which is faster but less reliable than TCP 3. References: 1: TCP/IP TCP, UDP, and IP protocols - IBM 2: Transport Layer | Layer 4 | The OSI-Model 3: TCP/IP Model vs. OSI Model | Similarities and Differences - Fortinet

NEW QUESTION # 83

Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?

- A. Path Vector
 - B. Split Horizon
 - C. Shortest Path
 - D. Hop Count

Answer: D

Explanation:

Routing Information Protocol (RIP) is an example of a distance-vector routing protocol that uses hop count as its routing metric. To prevent routing loops, in which packets effectively get stuck bouncing between various router nodes, RIP implements a hop limit of 15, which limits the size of networks that RIP can support. After a data packet crosses 15 router nodes (hops) between a source and a destination, the destination is considered unreachable.

NEW QUESTION # 84

• • • • •

We understand your itching desire of the exam. Do not be bemused about the exam. We will satisfy your aspiring goals. Our PCCP real questions are high efficient which can help you pass the exam during a week. We just contain all-important points of knowledge into our PCCP latest material. And we keep ameliorate our PCCP latest material according to requirements of PCCP exam. Besides, we arranged our PCCP Exam Prep with clear parts of knowledge. You may wonder whether our PCCP real questions are suitable for your current level of knowledge about computer, as a matter of fact, our PCCP exam prep applies to exam candidates of different degree. By practicing and remember the points in them, your review preparation will be highly effective and successful.

New PCCP Test Syllabus: <https://www.examdumpsvce.com/PCCP-valid-exam-dumps.html>

What's more, part of that ExamDumpsVCE PCCP dumps now are free: <https://drive.google.com/open?id=1twYPvT3O7Fann1-n2xsDhwunQ0Po03Ld>