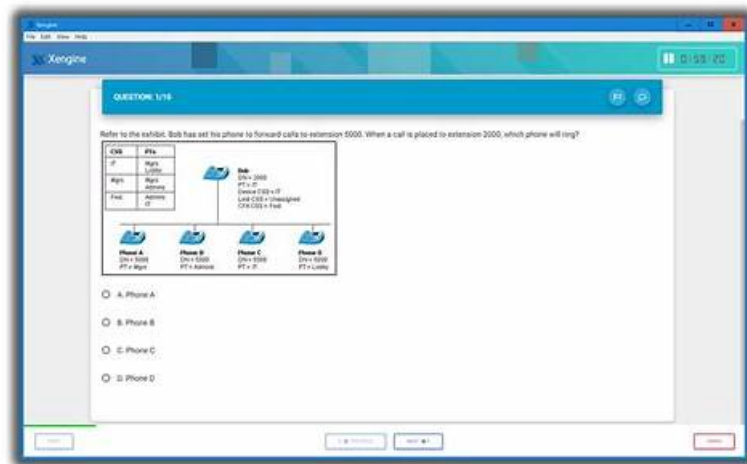


New PCCP Exam Simulator - PCCP Valid Test Prep



P.S. Free 2026 Palo Alto Networks PCCP dumps are available on Google Drive shared by Test4Cram:
<https://drive.google.com/open?id=1NOB7w2uvkwvBaaKxJvjhgHcwghGu2Mpy>

There are some prominent features that are making the PCCP exam dumps the first choice of PCCP certification exam candidates. The prominent features are real and verified Palo Alto Networks Certified Cybersecurity Practitioner exam questions, availability of PCCP exam dumps in three different formats, affordable price, 1 year free updated PCCP Exam Questions download facility, and 100 percent Palo Alto Networks PCCP exam passing money back guarantee. We are quite confident that all these PCCP exam dumps feature you will not find anywhere. Just download the Palo Alto Networks PCCP Certification Exams and start this journey right now.

Palo Alto Networks PCCP Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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 3	<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 4	<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.
---------	--

>> New PCCP Exam Simulator <<

Palo Alto Networks PCCP Valid Test Prep & PCCP Official Cert Guide

We will continue to pursue our passion for better performance and human-centric technology of latest PCCP quiz prep. And we guarantee you to pass the PCCP exam for we have confidence to make it with our technological strength. A good deal of researches has been made to figure out how to help different kinds of candidates to get the PCCP Certification. We have made classification to those faced with various difficulties, aiming at which we adopt corresponding methods. According to the statistics shown in the feedback chart, the general pass rate for latest PCCP test prep is 98%.

Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q63-Q68):

NEW QUESTION # 63

What is an event-driven snippet of code that runs on managed infrastructure?

- A. Serverless function
- B. API
- C. Docker container
- D. Hypervisor

Answer: A

Explanation:

A serverless function is an event-driven snippet of code that runs on managed infrastructure, typically as part of a Function as a Service (FaaS) model. It is executed in response to events such as HTTP requests or database changes, and the cloud provider handles the underlying infrastructure.

NEW QUESTION # 64

The customer is responsible only for which type of security when using a SaaS application?

- A. infrastructure
- B. platform
- C. data
- D. physical

Answer: C

Explanation:

Data security is the only type of security that the customer is fully responsible for when using a SaaS application. Data security refers to the protection of data from unauthorized access, use, modification, deletion, or disclosure. Data security includes aspects such as encryption, backup, recovery, access control, and compliance¹². The customer is responsible for ensuring that their data is secure in transit and at rest, and that they comply with any applicable regulations or policies regarding their data.

The other types of security - physical, platform, and infrastructure - are the responsibility of the SaaS provider. Physical security refers to the protection of the hardware and facilities that host the SaaS application. Platform security refers to the protection of the software and services that run the SaaS application. Infrastructure security refers to the protection of the network and systems that support the SaaS application. The SaaS provider is responsible for ensuring that these layers of security are maintained and updated, and that they meet the required standards and certifications³⁴. References:

- * SaaS and the Shared Security Model
- * A Guide to SaaS Shared Responsibility Model
- * The Shared Responsibility Model for Security in The Cloud (IaaS, PaaS & SaaS)
- * Shared responsibility in the cloud

NEW QUESTION # 65

Which option is a Prisma Access security service?

- **A. Firewall as a Service (FWaaS)**
- B. Compute Security
- C. Virtual Private Networks (VPNs)
- D. Software-defined wide-area networks (SD-WANs)

Answer: A

Explanation:

Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

NEW QUESTION # 66

Under which category does an application that is approved by the IT department, such as Office 365, fall?

- A. tolerated
- B. unsanctioned
- C. prohibited
- **D. sanctioned**

Answer: D

Explanation:

A sanctioned application is an application that is approved by the IT department and meets the security and compliance requirements of the organization. Sanctioned applications are allowed to access the organization's network and data and are monitored and protected by the IT department. Examples of sanctioned applications are Office 365, Salesforce, and Zoom. Sanctioned applications are different from unsanctioned, prohibited, and tolerated applications, which are not approved by the IT department and may pose security risks to the organization. Unsanctioned applications are applications that are used by the employees without the IT department's knowledge or consent, such as Dropbox, Gmail, or Facebook. Prohibited applications are applications that are explicitly forbidden by the IT department, such as BitTorrent, Tor, or malware. Tolerated applications are applications that are not approved by the IT department, but are not blocked or restricted, such as Skype, Spotify, or YouTube. References: Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), Cloud Security Fundamentals - Module 4: Cloud Security Best Practices, Application Visibility and Control

NEW QUESTION # 67

Which statement describes a host-based intrusion prevention system (HIPS)?

- A. It analyzes network traffic to detect unusual traffic flows and new malware.
- **B. It is installed on an endpoint and inspects the device.**
- C. It is placed as a sensor to monitor all network traffic and scan for threats.
- D. It scans a Wi-Fi network for unauthorized access and removes unauthorized devices.

Answer: B

Explanation:

A Host-Based Intrusion Prevention System (HIPS) is installed directly on an endpoint device (such as a server or workstation) and monitors local system activity, including processes, file access, and system calls, to detect and prevent malicious behavior.

• • • • •

PCCP Valid Test Prep: https://www.test4cram.com/PCCP_real-exam-dumps.html

- P.S. Free 2026 Palo Alto Networks PCCP dumps are available on Google Drive shared by Test4Cram: <https://drive.google.com/open?id=1NOB7w2uvkwBaaKxJvjhgHcwghGu2Mpy>