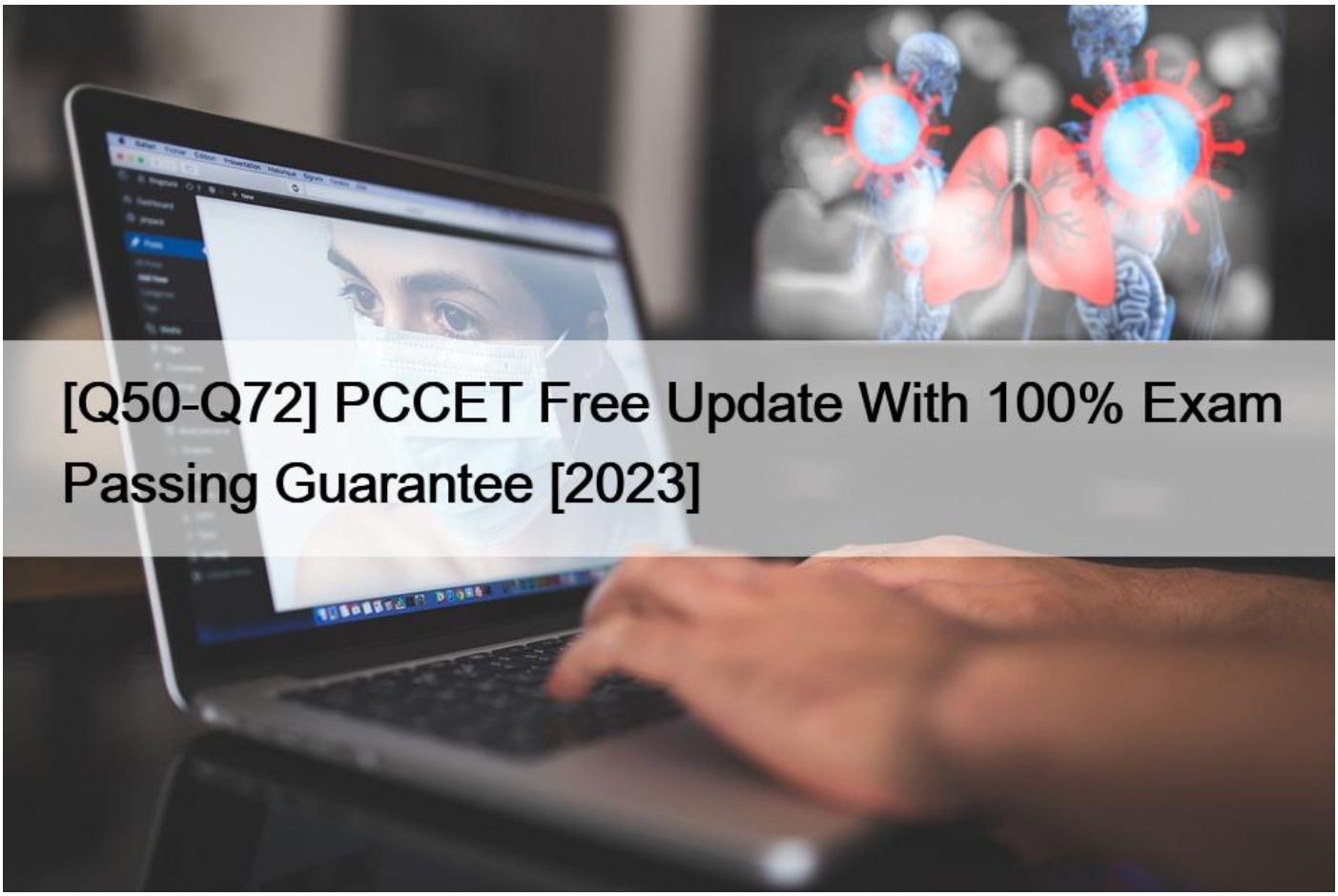
[Q50-Q72 PCCET Free Update With 100% Exam Passing Guarantee [2023



PCCET Free Update With 100% Exam Passing Guarantee [2023]
[Apr-2023] Verified Palo Alto Networks Exam Dumps with PCCET Exam Study Guide

Where can I take Palo Alto Networks PCCET Certification Exam?

You can take the exam anywhere in the world by signing up for an exam voucher. After you sign up for a test voucher, you will receive a unique link that you can use to schedule your Palo Alto Networks PCCET certification exam. You can schedule your exam at any time within 60 days of receiving your test voucher. **PCCET Dumps** will cover all exam related costs including the exam fee. The candidate can also take the Palo Alto Networks PCCET Certification Exam via a third-party testing service provider like TestPlant or VUE Test Center. Candidates are expected to pay for the test fees in advance. Candidates who are unable to take the exam through the voucher system can purchase the test via the VUE Test Center.

Palo Alto PCCET Exam Certification Details:

Passing ScoreVariable (70-80 / 100 Approx.)Exam Price$110 USDDuration90 minutesExam NameCybersecurity Entry-level TechnicianExam RegistrationPEARSON VUE

Q50. In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?
* Cortex XDR
* AutoFocus
* MineMild
* Cortex XSOAR

In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.

Q51. What is the purpose of SIEM?
* Securing cloud-based applications
* Automating the security team’s incident response
* Real-time monitoring and analysis of security events
* Filtering webpages employees are allowed to access

Q52. Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?
* Threat Prevention
* DNS Security
* WildFire
* URL Filtering

The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

Q53. Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?
* Group policy
* Stateless
* Stateful
* Static packet-filter

Explanation

Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics:

They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks.

They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules.

After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session.

This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren’t inspected after the connection is established.

Q54. Which statement is true about advanced persistent threats?

* They use script kiddies to carry out their attacks.
* They have the skills and resources to launch additional attacks.
* They lack the financial resources to fund their activities.
* They typically attack only once.

Q55. 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?
* User-ID
* Lightweight Directory Access Protocol (LDAP)
* User and Entity Behavior Analytics (UEBA)
* Identity and Access Management (IAM)

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.

Q56. If an endpoint does not know how to reach its destination, what path will it take to get there?
* The endpoint will broadcast to all connected network devices.
* The endpoint will not send the traffic until a path is clarified.
* The endpoint will send data to the specified default gateway.
* The endpoint will forward data to another endpoint to send instead.

Q57. What are three benefits of SD-WAN infrastructure? (Choose three.)
* Improving performance of SaaS applications by requiring all traffic to be back-hauled through the corporate headquarters network
* Promoting simplicity through the utilization of a centralized management structure
* Utilizing zero-touch provisioning for automated deployments
* Leveraging remote site routing technical support by relying on MPLS
* Improving performance by allowing efficient access to cloud-based resources without requiring back-haul traffic to a centralized location

Explanation

Simplicity: Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites. Improved performance: By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.

Q58. Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?
* Statistical-based
* Knowledge-based
* Behavior-based
* Anomaly-based

A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.

* A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.

These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

Q59. Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?
* endpoint antivirus software
* strong endpoint passwords
* endpoint disk encryption
* endpoint NIC ACLs

Q60. What differentiates knowledge-based systems from behavior-based systems?
* Behavior-based systems find the data that knowledge-based systems store.
* Knowledge-based systems pull from a previously stored database that distinguishes “bad”. C.

Knowledge-based systems try to find new, distinct traits to find “bad” things.
* Behavior-based systems pull from a previously stored database that distinguishes “bad”.

Q61. You have been invited to a public cloud design and architecture session to help deliver secure east west flows and secure Kubernetes workloads.

What deployment options do you have available? (Choose two.)
* PA-Series
* VM-Series
* Panorama
* CN-Series

Q62. What type of DNS record maps an IPV6 address to a domain or subdomain to another hostname?
* SOA
* NS
* AAAA
* MX

Q63. What is the primary security focus after consolidating data center hypervisor hosts within trust levels?
* control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
* control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
* control and protect inter-host traffic by using IPv4 addressing
* control and protect inter-host traffic using physical network security appliances

Explanation

page 211 “Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: … … … This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus.”

Q64. Which feature of the VM-Series firewalls allows them to fully integrate into the DevOps workflows and CI/CD pipelines without slowing the pace of business?
* Elastic scalability
* 5G
* External dynamic lists
* Log export

Q65. Which tool supercharges security operations center (SOC) efficiency with the world’s most comprehensive operating platform for enterprise security?
* Prisma SAAS
* WildFire
* Cortex XDR
* Cortex XSOAR

Q66. Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?
* Shortest Path
* Hop Count
* Split Horizon
* Path Vector

Q67. Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?
* Global Protect
* WildFire
* AutoFocus
* STIX

page 173 “AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities.”

Q68. Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?
* Session, Transport, Network
* Application, Presentation, and Session
* Physical, Data Link, Network
* Data Link, Session, Transport

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model.

Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.

Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.

Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

Q69. Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?
* Network
* Management
* Cloud
* Security

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

* Networking

* Software-defined wide-area networks (SD-WANs)

* Virtual private networks (VPNs)

* Zero Trust network access (ZTNA)

* Quality of Service (QoS)

* Security

* Firewall as a service (FWaaS)

* Domain Name System (DNS) security

* Threat prevention

* Secure web gateway (SWG)

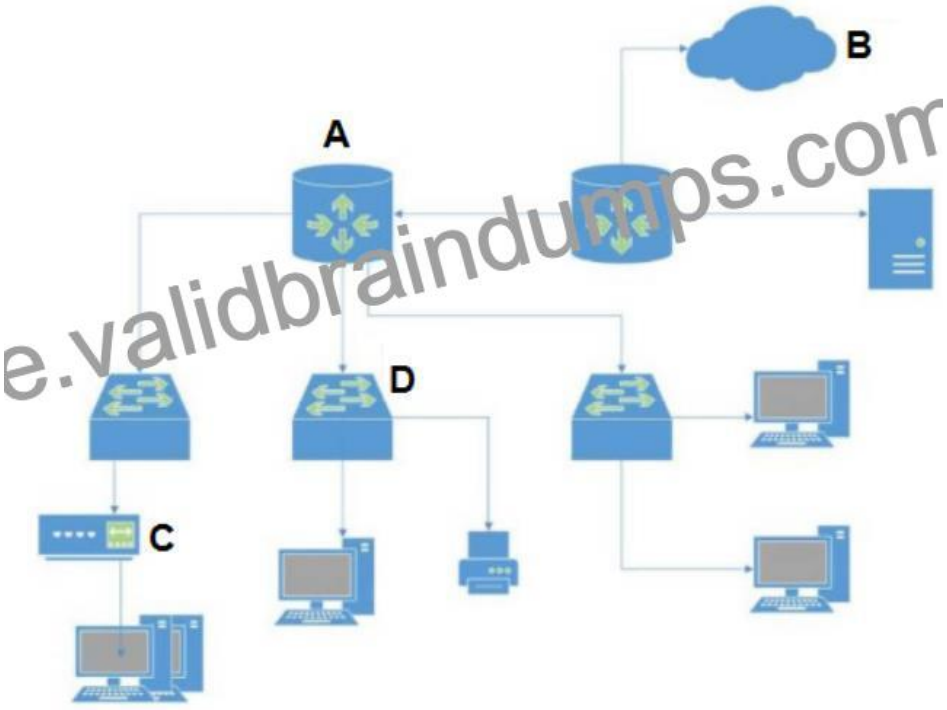
* Data loss prevention (DLP)

* Cloud access security broker (CASB)

Q70. Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?
* DNS Security
* URL Filtering
* WildFire
* Threat Prevention

Q71. Which type of malware replicates itself to spread rapidly through a computer network?
* ransomware
* Trojan horse
* virus
* worm
A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

Q72. In the network diagram below, which device is the router?



* A
* C
* D
* B

Authentic Best resources for PCCET Online Practice Exam: https://www.validbraindumps.com/PCCET-exam-prep.html]