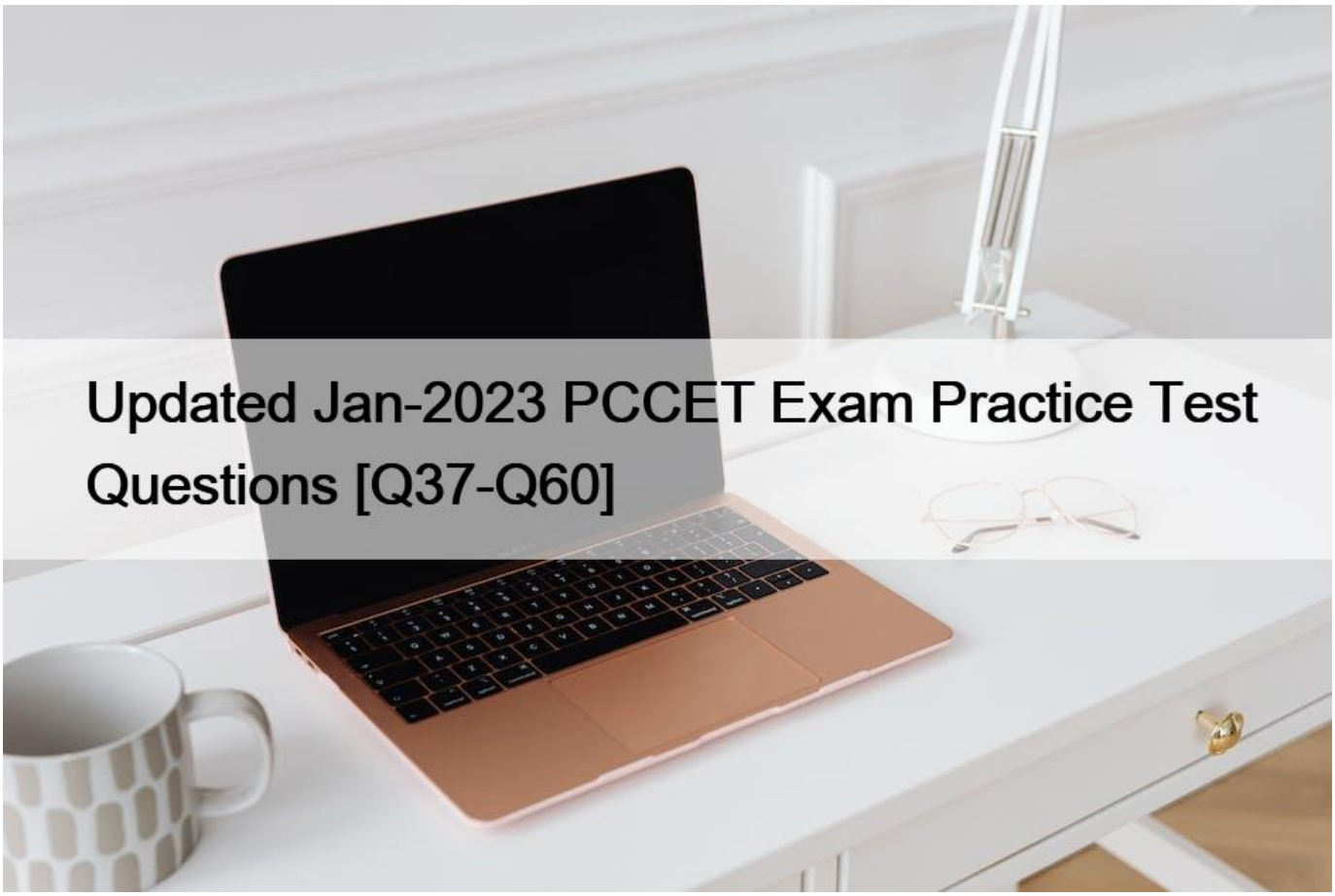
Updated Jan-2023 PCCET Exam Practice Test Questions [Q37-Q60



Updated Jan-2023 PCCET Exam Practice Test Questions
Verified PCCET dumps Q&As 100% Pass in First Attempt Guaranteed Updated Dump

Palo Alto PCCET Exam Certification Details:

Exam RegistrationPEARSON VUEPassing ScoreVariable (70-80 / 100 Approx.)Number of Questions75Sample QuestionsPalo Alto PCCET Sample QuestionsExam Price$110 USDExam CodePCCETRecommended TrainingIntroduction to Cybersecurity

Fundamentals of Network Security

Fundamentals of Cloud Security

Fundamentals of SOC (Security Operations Center)Duration90 minutes

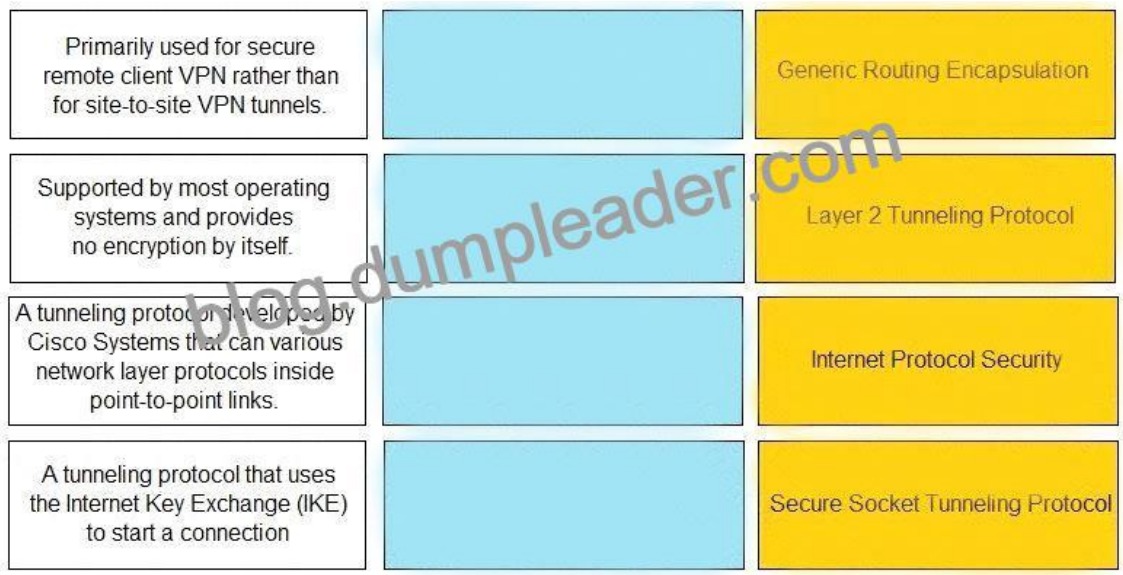
Here is the importance of taking the Palo Alto Networks PCCET Certification Exam:

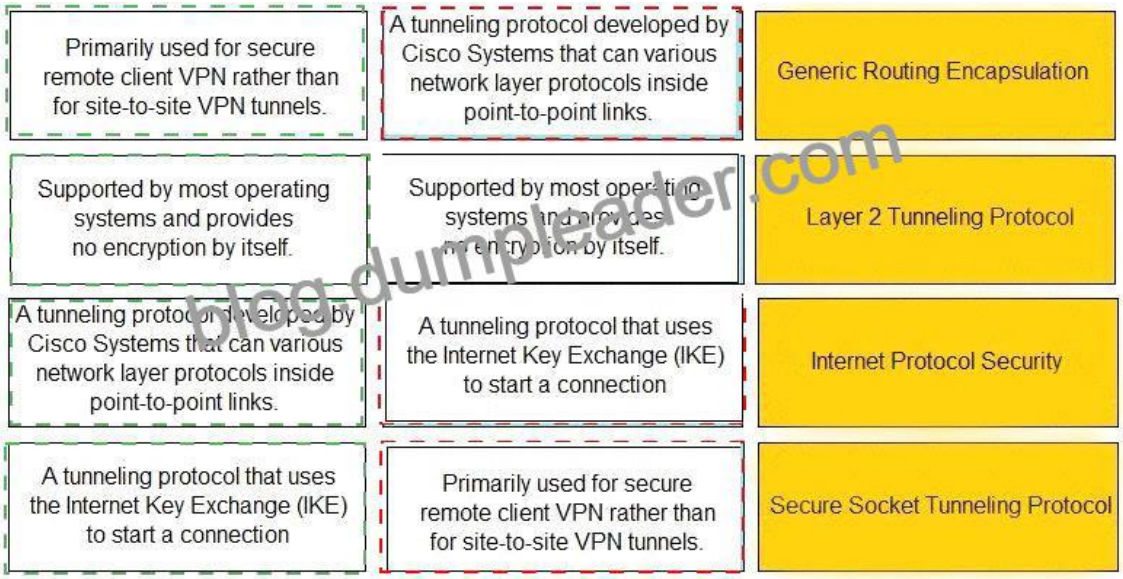
In the current era of the ever-evolving threat landscape, it is crucial to have a basic understanding of the foundational knowledge of the cybersecurity field. In this context, the PCCET certification exam serves as a starting point for candidates who are looking to

enter the cybersecurity field or who want to validate their existing cybersecurity knowledge. The certification is based on the NIST/NICE framework. **PCCET Dumps** is a comprehensive and accurate tool that allows students to test their skills and gain certification from one of the leading cybersecurity vendors. This framework is designed to align with the latest cybersecurity curriculum and help ensure that students acquire the required skills.
Furthermore, this certification aims to validate candidates' fundamental cybersecurity, network security, cloud security, and SOC security knowledge through an online examination. Upon completion of the exam, candidates will receive a certificate that verifies their understanding of the core concepts, principles, and practices of the cybersecurity field. In addition to the certificate, all candidates will also receive a score based on their performance on the test.

Q37. 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

Q38. Match the description with the VPN technology.





Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.	Supported by most operating systems and provides no encryption by itself.	Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

Q39. How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

* DevSecOps improves pipeline security by assigning the security team as the lead team for continuous deployment
* DevSecOps ensures the pipeline has horizontal intersections for application code deployment
* DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
* DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

Q40. Which type of LAN technology is being displayed in the diagram?

* Star Topology
* Spine Leaf Topology
* Mesh Topology
* Bus Topology

Q41. 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
“The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention”

Q42. A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.

Which NIST cloud service model is this?
* IaaS
* SaaS
* PaaS
* CaaS
SaaS – User responsible for only the data, vendor responsible for rest

Q43. 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
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.

Q44. Which aspect of a SaaS application requires compliance with local organizational security policies?
* Types of physical storage media used
* Data-at-rest encryption standards
* Acceptable use of the SaaS application
* Vulnerability scanning and management

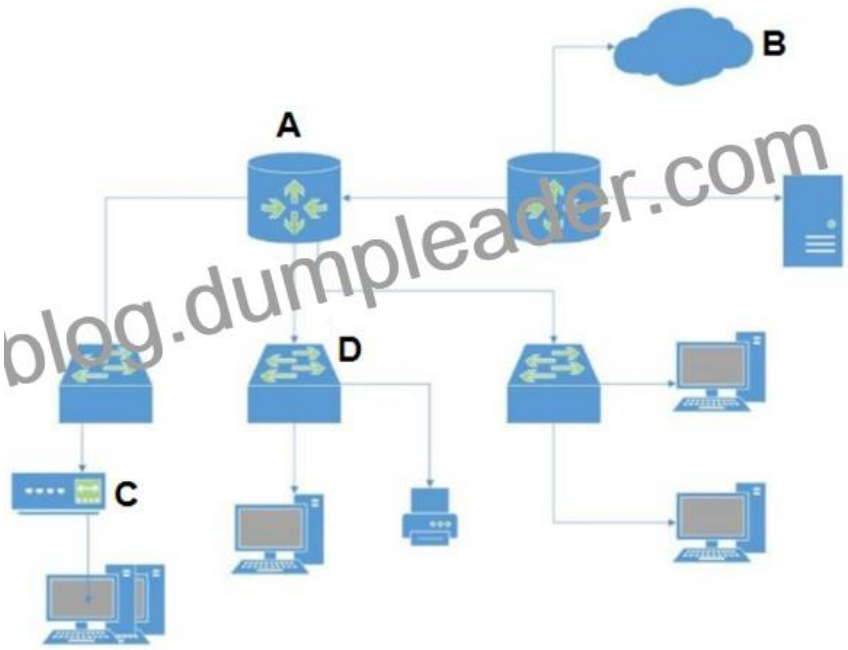
Q45. SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

* People
* Accessibility
* Processes
* Understanding
* Business

Q46. Which technique changes protocols at random during a session?
* use of non-standard ports
* port hopping
* hiding within SSL encryption
* tunneling within commonly used services

Port hopping, in which ports and protocols are randomly changed during a session.

Q47. In the attached network diagram, which device is the switch?



* A
* B
* C
* D

Q48. What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?
* run a static analysis
* check its execution policy
* send the executable to WildFire
* run a dynamic analysis

Q49. Which technique changes protocols at random during a session?
* use of non-standard ports
* port hopping
* hiding within SSL encryption

* tunneling within commonly used services

Q50. Which subnet does the host 192.168.19.36/27 belong?
* 192.168.19.0
* 192.168.19.16
* 192.168.19.64
* 192.168.19.32

Q51. Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?
* Cortex XSOAR
* Prisma Cloud
* AutoFocus
* Cortex XDR

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

https://www.paloaltonetworks.com/cortex/security-operations-automation

Q52. Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?
* MineMeld
* AutoFocus
* WildFire
* Cortex XDR

Q53. A native hypervisor runs:
* with extreme demands on network throughput
* only on certain platforms
* within an operating system’s environment
* directly on the host computer’s hardware

Q54. 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

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.”

Q55. 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)

Q56. Which method is used to exploit vulnerabilities, services, and applications?
* encryption
* port scanning
* DNS tunneling
* port evasion

Attack communication traffic is usually hidden with various techniques and tools, including:

* Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption

* Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic.

* Port evasion using network anonymizers or port hopping to traverse over any available open ports

* Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult

* DNS tunneling is used for C2 communications and data infiltration

Q57. SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)
* People
* Accessibility
* Processes
* Understanding
* Business

Explanation

Q58. Which characteristic of serverless computing enables developers to quickly deploy application code?
* Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
* Uploading the application code itself, without having to provision a full container image or any OS virtual machine components
* Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
* Using Container as a Service (CaaS) to deploy application containers to run their code.

Q59. 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.

Q60. 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

Following is the purpose of the Palo Alto Networks PCCET Certification Exam:

The purpose of the Palo Alto Networks PCCET certification exam is to provide candidates with a comprehensive understanding of the foundation concepts and principles in the cybersecurity field. The certification exam is based on the NIST/NICE framework. This framework is designed to align with the latest cybersecurity curriculum and help ensure that students acquire the required skills. The exam is designed to help candidates gain foundational knowledge of the cybersecurity field, such as understanding cyber threats and defenses, and cyber hygiene. It will also validate candidates' knowledge of network security, cloud security, and SOC security. Candidates must demonstrate the ability to identify various cyber threats and defenses as well as to implement secure network design and configuration.