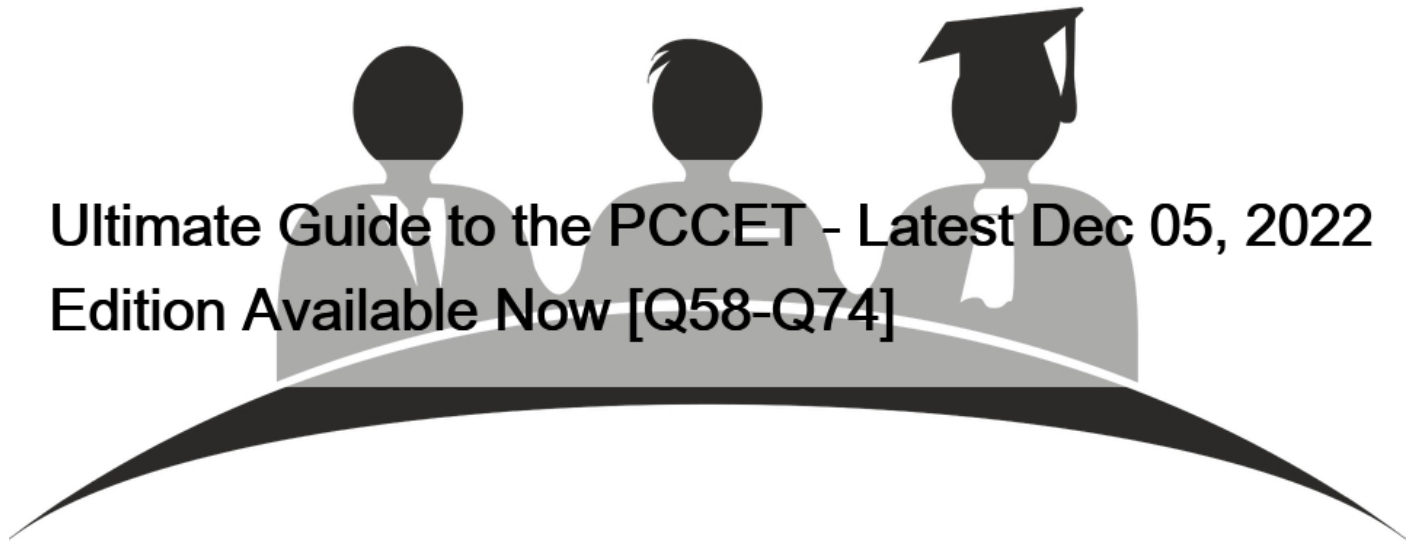# Ultimate Guide to the PCCET - Latest Dec 05, 2022 Edition Available Now [Q58-Q74

Ultimate Guide to the PCCET - Latest Dec 05, 2022 Edition Available Now
2022 Updated Verified Pass PCCET Exam - Real Questions and Answers

Targeted audience for the Palo Alto Networks PCCET Certification Exam:
The PCCET certification exam is designed for technical professionals, students, and non-technical individuals interested in validating comprehensive knowledge on current cybersecurity tenets. Candidates must be able to demonstrate the ability to understand how cyber threats manifest themselves, where they originate, and what the right defenses are to stop them. Candidates must be able to identify various cyber threats and defenses as well as to implement secure network design and configuration. Candidates should have basic knowledge of networking and security technologies and concepts. Logical addresses must be used, and they should understand how networks operate.

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.

NO.58 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)

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.

NO.59 Which IPsec feature allows device traffic to go directly to the Internet?
* Split tunneling
* Diffie-Hellman groups
* d.Authentication Header (AH)
* IKE Security Association

“Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation.”

NO.60 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”

NO.61 Which key component is used to configure a static route?
* router ID
* enable setting
* routing protocol
* next hop IP address

NO.62 Match the description with the VPN technology.

Description		VPN Technology
Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.		Generic Routing Encapsulation
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.		Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection		Secure Socket Tunneling Protocol

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

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

NO.63 Under which category does an application that is approved by the IT department, such as Office 365, fall?

* unsanctioned
* prohibited
* tolerated
* sanctioned

NO.64 The customer is responsible only for which type of security when using a SaaS application?

* physical
* platform
* data
* infrastructure

NO.65 In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across

the internet so that they can modify their attack objectives and methods?

* exploitation
* actions on the objective
* command and control
* installation

Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

NO.66 Why is it important to protect East-West traffic within a private cloud?

* All traffic contains threats, so enterprises must protect against threats across the entire network
* East-West traffic contains more session-oriented traffic than other traffic
* East-West traffic contains more threats than other traffic
* East-West traffic uses IPv6 which is less secure than IPv4

NO.67 Which type of LAN technology is being displayed in the diagram?
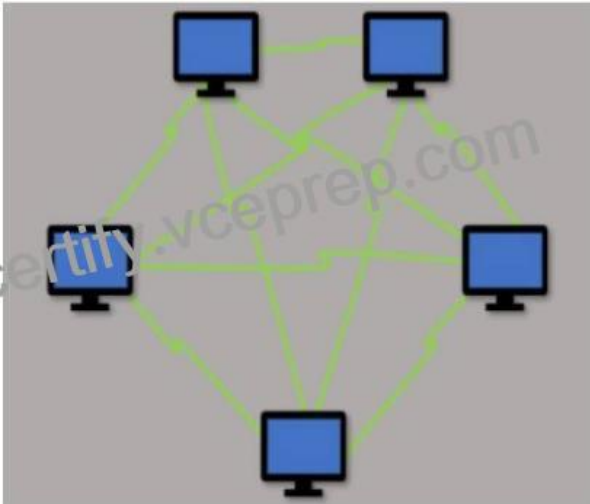
* Star Topology
* Spine Leaf Topology
* Mesh Topology
* Bus Topology

NO.68 Which IoT connectivity technology is provided by satellites?

* 4G/LTE
* VLF
* L-band
* 2G/2.5G

NO.69 Given the graphic, match each stage of the cyber-attack lifecycle to its description.

reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

NO.70 During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?
* Frame
* Segment
* Packet
* Data

The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.

NO.71 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.

NO.72 Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?
* North-South traffic
* Intrazone traffic
* East-West traffic
* Interzone traffic

NO.73 Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?
* Shortest Path
* Hop Count
* Split Horizon
* Path Vector

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.

NO.74 In SecOps, what are two of the components included in the identify stage? (Choose two.)
* Initial Research
* Change Control
* Content Engineering
* Breach Response

Dumps Moneyack Guarantee - PCCET Dumps Approved Dumps: https://www.vceprep.com/PCCET-latest-vce-prep.html]