

# Paloalto-Networks

## Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician



#### NEW QUESTION 1

Match the Identity and Access Management (IAM) security control with the appropriate definition.

IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

#### NEW QUESTION 2

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

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

**Answer:** C

#### NEW QUESTION 3

In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

- A. the network is large  
B. the network is small  
C. the network has low bandwidth requirements  
D. the network needs backup routes

**Answer:** A

**Explanation:**

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

#### NEW QUESTION 4

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?

- A. exploitation
- B. actions on the objective
- C. command and control
- D. installation

**Answer:** C

**Explanation:**

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.

**NEW QUESTION 5**

Why have software developers widely embraced the use of containers?

- A. Containers require separate development and production environments to promote authentic code.
- B. Containers share application dependencies with other containers and with their host computer.
- C. Containers simplify the building and deploying of cloud native applications.
- D. Containers are host specific and are not portable across different virtual machine hosts.

**Answer:** C

**NEW QUESTION 6**

Match each description to a Security Operating Platform key capability.

understanding the full context of attacks on a network		detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications		provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack		prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people		reduce the attack surface area

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.

Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats.

Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the various security solutions in the organization’s environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

**NEW QUESTION 7**

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- A. weaponization
- B. reconnaissance
- C. exploitation
- D. delivery

**Answer:** A

**Explanation:**

"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

**NEW QUESTION 8**

Which core component is used to implement a Zero Trust architecture?

- A. VPN Concentrator
- B. Content Identification
- C. Segmentation Platform
- D. Web Application Zone

**Answer:** C

**Explanation:**

"Remember that a trust zone is not intended to be a "pocket of trust" where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that all communications traffic, including traffic between devices in the same zone, is intermediated by the corresponding Zero Trust Segmentation Platform."

**NEW QUESTION 9**

Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

- A. Expedition
- B. Cortex XDR
- C. AutoFocus
- D. App-ID

**Answer:** B

**NEW QUESTION 10**

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. Credit card number
- B. Trade secret
- C. National security information
- D. A symmetric encryption key

**Answer:** A

**NEW QUESTION 10**

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

- A. XDR
- B. STEP
- C. SOAR
- D. SIEM

**Answer:** C

**NEW QUESTION 15**

Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

- A. Benign
- B. Tolerated
- C. Sanctioned
- D. Secure

**Answer:** C

**NEW QUESTION 18**

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

- A. Cortex XSOAR
- B. Prisma Cloud
- C. AutoFocus
- D. Cortex XDR

**Answer:** A

**Explanation:**

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>

**NEW QUESTION 19**

What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

- A. run a static analysis
- B. check its execution policy
- C. send the executable to WildFire
- D. run a dynamic analysis

**Answer:** B

**NEW QUESTION 20**

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

- A. Network
- B. Management
- C. Cloud
- D. Security

**Answer:** D

**Explanation:**

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)

**NEW QUESTION 22**

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Unordered Options

Presentation

Application

Physical

Transport

Session

Network

Data Link

Ordered Options

↔

↕

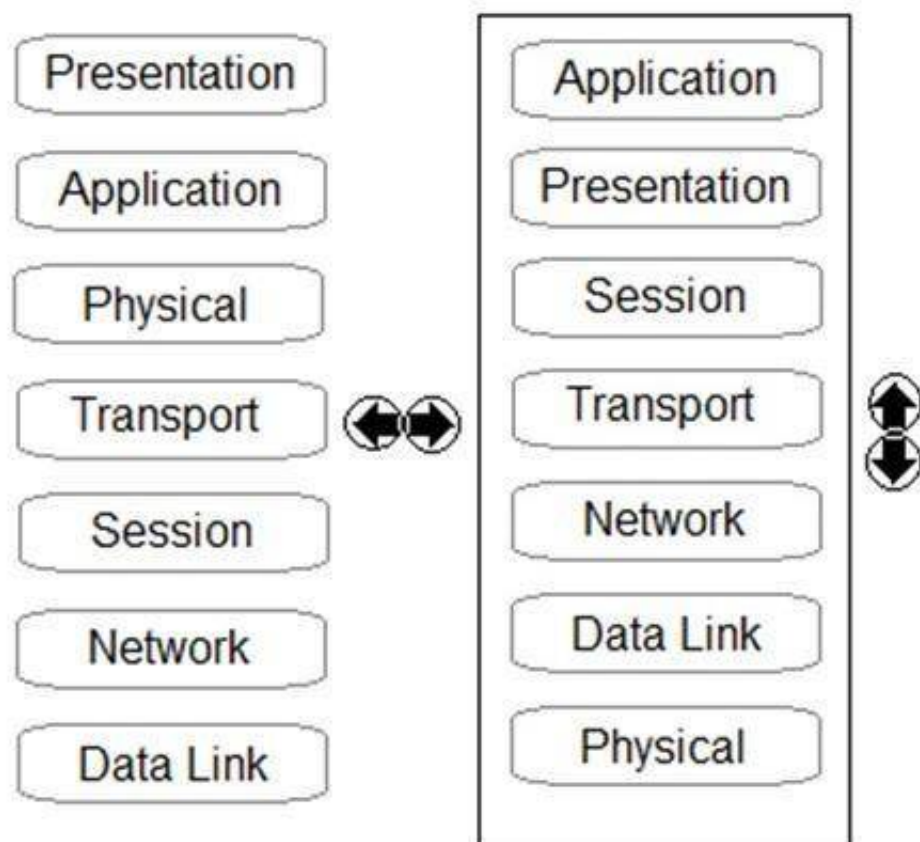
- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



## Unordered Options      Ordered Options



### NEW QUESTION 27

Which pillar of Prisma Cloud application security does vulnerability management fall under?

- A. dynamic computing
- B. identity security
- C. compute security
- D. network protection

**Answer: C**

#### Explanation:

Prisma Cloud comprises four pillars:

Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.

Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.

Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.

Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

### NEW QUESTION 32

Which network device breaks networks into separate broadcast domains?

- A. Hub
- B. Layer 2 switch
- C. Router
- D. Wireless access point

**Answer: C**

#### Explanation:

A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

### NEW QUESTION 35

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?

- A. DNS Security
- B. URL Filtering
- C. WildFire
- D. Threat Prevention

**Answer: C**

#### Explanation:

"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"

**NEW QUESTION 36**

How does adopting a serverless model impact application development?

- A. costs more to develop application code because it uses more compute resources
- B. slows down the deployment of application code, but it improves the quality of code development
- C. reduces the operational overhead necessary to deploy application code
- D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

**Answer:** C

**Explanation:**

List three advantages of serverless computing over CaaS: - Reduce costs - Increase agility - Reduce operational overhead

**NEW QUESTION 38**

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

- A. NetOps
- B. SecOps
- C. SecDevOps
- D. DevOps

**Answer:** B

**Explanation:**

Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

**NEW QUESTION 43**

Which method is used to exploit vulnerabilities, services, and applications?

- A. encryption
- B. port scanning
- C. DNS tunneling
- D. port evasion

**Answer:** D

**Explanation:**

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

**NEW QUESTION 45**

Match the description with the 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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 49

Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

- A. MineMeld
- B. AutoFocus
- C. WildFire
- D. Cortex XDR

**Answer:** B

**Explanation:**

"Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."

#### NEW QUESTION 53

Which type of malware replicates itself to spread rapidly through a computer network?

- A. ransomware
- B. Trojan horse
- C. virus
- D. worm

**Answer:** D

**Explanation:**

A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

#### NEW QUESTION 58

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- A. operating system patches
- B. full-disk encryption
- C. periodic data backups
- D. endpoint-based firewall

**Answer:** B

#### NEW QUESTION 59

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

- A. Cortex XDR
- B. AutoFocus
- C. MineMild
- D. Cortex XSOAR

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 61

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



- A. People
- B. Accessibility
- C. Processes
- D. Understanding
- E. Business

**Answer:** ACE

**Explanation:**

The six pillars include:

- \* 1. Business (goals and outcomes)
- \* 2. People (who will perform the work)
- \* 3. Interfaces (external functions to help achieve goals)
- \* 4. Visibility (information needed to accomplish goals)
- \* 5. Technology (capabilities needed to provide visibility and enable people)
- \* 6. Processes (tactical steps required to execute on goals)

All elements must tie back to the business itself and the goals of the security operations

**NEW QUESTION 63**

Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

- A. Session, Transport, Network
- B. Application, Presentation, and Session
- C. Physical, Data Link, Network
- D. Data Link, Session, Transport

**Answer:** B

**Explanation:**

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

**NEW QUESTION 64**

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

- A. Dynamic
- B. Pre-exploit protection
- C. Bare-metal
- D. Static

**Answer:** A

**Explanation:**

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.

**NEW QUESTION 69**

Which pillar of Prisma Cloud application security addresses ensuring that your cloud resources and SaaS applications are correctly configured?

- A. visibility, governance, and compliance
- B. network protection
- C. dynamic computing
- D. compute security

**Answer:** A

**Explanation:**

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

**NEW QUESTION 74**

Which subnet does the host 192.168.19.36/27 belong?

- A. 192.168.19.0
- B. 192.168.19.16
- C. 192.168.19.64
- D. 192.168.19.32

**Answer:** D

**NEW QUESTION 77**

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?

- A. Group policy
- B. Stateless
- C. Stateful
- D. Static packet-filter

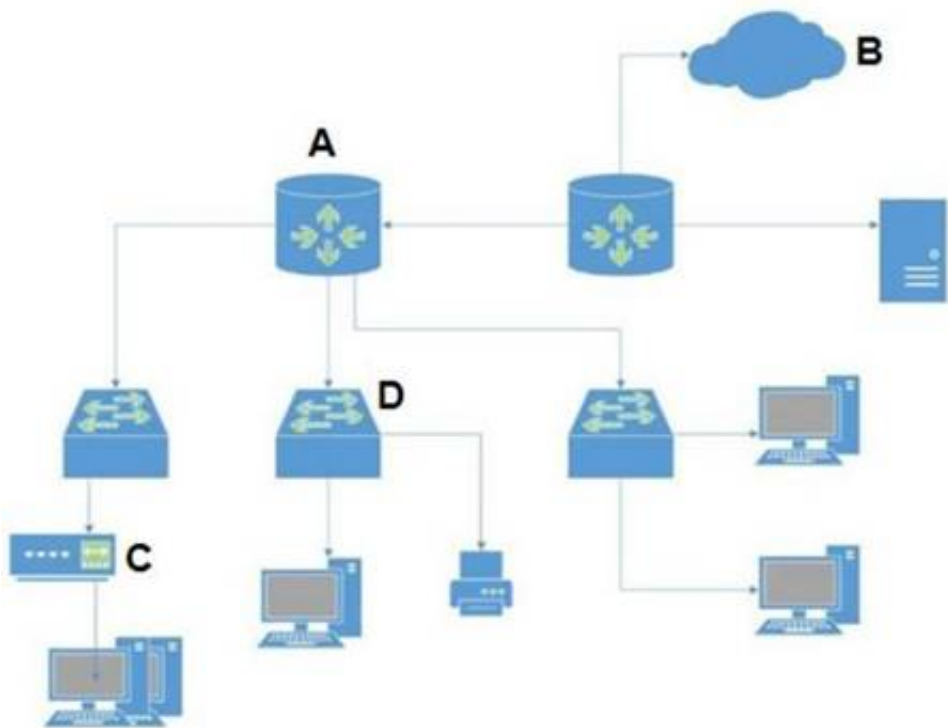
Answer: C

**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.

**NEW QUESTION 81**

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



- A. A
- B. B
- C. C
- D. D

Answer: D

**NEW QUESTION 83**

Match the Palo Alto Networks WildFire analysis verdict with its definition.

Answer Area

Benign

Grayware

Malware

malicious in intent and can pose a security threat

does not pose a direct security threat

does not exhibit a malicious behavior

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Benign: Safe and does not exhibit malicious behavior

Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)

Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits)

Phishing: Malicious attempt to trick the recipient into revealing sensitive data

**NEW QUESTION 85**

Which option is an example of a North-South traffic flow?

- A. Lateral movement within a cloud or data center
- B. An internal three-tier application
- C. Client-server interactions that cross the edge perimeter
- D. Traffic between an internal server and internal user

**Answer: C**

**Explanation:**

North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.

**NEW QUESTION 87**

Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

- A. User-ID
- B. Device-ID
- C. App-ID
- D. Content-ID

**Answer: C**

**Explanation:**

App-ID™ technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

**NEW QUESTION 92**

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?

- A. IaaS
- B. SaaS
- C. PaaS
- D. CaaS

**Answer: B**

**Explanation:**

SaaS - User responsible for only the data, vendor responsible for rest

**NEW QUESTION 97**

Which network analysis tool can be used to record packet captures?

- A. Smart IP Scanner
- B. Wireshark
- C. Angry IP Scanner
- D. Netman

**Answer: B**

**NEW QUESTION 101**

Which IPsec feature allows device traffic to go directly to the Internet?

- A. Split tunneling
- B. Diffie-Hellman groups
- C. d.Authentication Header (AH)
- D. IKE Security Association

**Answer: A**

**Explanation:**

"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."

**NEW QUESTION 102**

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

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


**Answer:** B


**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 103**


Given the graphic, match each stage of the cyber-attack lifecycle to its description.


  
**1**

  
**2**

  
**3**

  
**4**

  
**5**

  
**6**

Unauthorized Access

Unauthorized Use

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



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

#### NEW QUESTION 105

What is required for a SIEM to operate correctly to ensure a translated flow from the system of interest to the SIEM data lake?

- A. connectors and interfaces
- B. infrastructure and containers
- C. containers and developers
- D. data center and UPS

**Answer:** A

#### NEW QUESTION 106

Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

- A. Prisma SAAS
- B. WildFire
- C. Cortex XDR
- D. Cortex XSOAR

**Answer:** D

#### Explanation:

Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering.

#### NEW QUESTION 109

Which option is a Prisma Access security service?

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

**Answer:** B

#### 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 110

In a traditional data center what is one result of sequential traffic analysis?

- A. simplifies security policy management
- B. reduces network latency
- C. causes security policies to be complex
- D. improves security policy application ID enforcement

**Answer:** C

**Explanation:**

Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying

**NEW QUESTION 115**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### PCCET Practice Exam Features:

- \* PCCET Questions and Answers Updated Frequently
- \* PCCET Practice Questions Verified by Expert Senior Certified Staff
- \* PCCET Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PCCET Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PCCET Practice Test Here](#)**