Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

PCCSA Dumps
PCCSA Braindumps
PCCSA Real Questions
PCCSA Practice Test
PCCSA Actual Questions


killexams.com

**Palo-Alto**

# PCCSA

*Palo Alto Networks Certified Cybersecurity Associate*


ORDER FULL VERSION

Question #671

Which type of firewall monitors traffic streams from beginning to end?

- A. circuit-level gateway
- B. stateless
- C. stateful
- D. packet filter

**Answer:** C

Question #672

Which option lists the correct sequence of a TCP three-way handshake?

- A. SYN, ACK, SYN
- B. SYN, SYN+ACK, ACK
- C. SYN, ACK, FIN
- D. SYN, SYN+ACK, FIN

**Answer:** B

Question #673

Which two types of SaaS applications are allowed by an IT department? (Choose two.)

- A. tolerated
- B. certified
- C. sanctioned
- D. unsanctioned

**Answer:** AC
Reference:
https://www.paloaltonetworks.com/cyberpedia/saas-security

Question #674

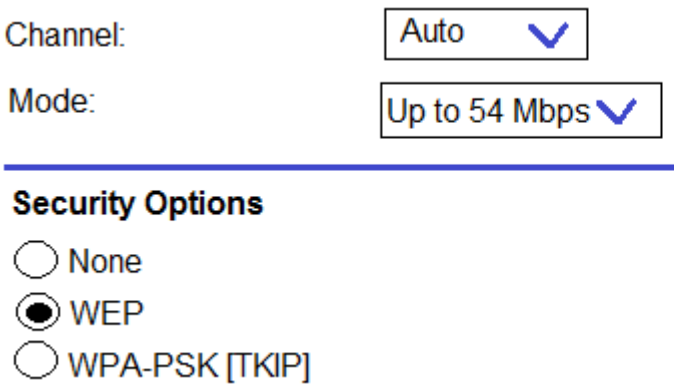
Which network method securely connects two sites across a public network?

- A. VPN
- B. VLAN
- C. switch
- D. router

**Answer:** A

Question #675

Review the exhibit and identify the type of vulnerability or attack that is commonly used against this technology.




- A. phishing
- B. denial-of-service
- C. code-injection
- D. password cracking

**Answer:** D

Question #676

When accessing an intranet website, a certificate error is received. What can be done to move past the certificate error and ensure that the error is not received the next time the website is accessed?

- A. install the website certificate into the web browser
- B. request trusted access from the web developer
- C. enable TLS 2.0 in the advanced options of the web browser
- D. trust the web developer for the application

**Answer:** A

Question #677

Assume that it is your responsibility to secure the software functioning at all layers in the exhibit.
Which cloud service model type is represented?


- A. software as a service
- B. platform as a service
- C. infrastructure as a service
- D. on-premises

**Answer:** D

Question #678

Which security principle describes the practice of giving users the minimum rights to access the resources necessary to do their jobs?

- A. known privilege
- B. least privilege
- C. user privilege
- D. lowest privilege

**Answer:** B

**Question: 679**

In securing east-west traffic within a microservices architecture, which of the following approaches is most beneficial for maintaining security without compromising the agility of development teams?

A. Implementing a strict firewall at the service level
B. Enforcing network segmentation at all layers
C. Utilizing service mesh technology for traffic management
D. Establishing a centralized security operations center

Answer: C

Explanation: Service mesh technology provides a lightweight and efficient way to manage secure communication between microservices, allowing for agility while maintaining robust security controls.

**Question: 680**

While conducting a security assessment, a team discovers that several employees have been using unsecured public Wi-Fi networks to access corporate resources. What is the best practice to mitigate the risks associated with using public Wi-Fi?

A. Require the use of a virtual private network (VPN) for all connections
B. Encourage employees to use personal devices only
C. Limit employee access to the internet
D. Disable all remote access to corporate resources

Answer: A

Explanation: Requiring the use of a virtual private network (VPN) for all connections helps encrypt data transmitted over public Wi-Fi, significantly reducing the risk of interception and unauthorized access to corporate resources.

**Question: 681**
Which of the following statements best describes the inherent risks associated with Software as a Service (SaaS) applications, particularly concerning data ownership and security?
A. SaaS applications always encrypt data in transit and at rest.
B. SaaS providers may have access to sensitive data, leading to privacy concerns.
C. Organizations retain full control over their data in SaaS solutions.
D. SaaS applications are immune to insider threats.

Answer: B

Explanation: SaaS providers may access sensitive data to provide services, which raises privacy and security concerns, especially regarding compliance with data protection regulations.

**Question: 682**
Which of the following explains the concept of "micro-segmentation" in a Zero Trust security environment?
A. Segmenting the network based on user roles only.
B. Allowing unrestricted access to certain network segments for ease of use.
C. Using a single perimeter firewall for all network segments.
D. Creating smaller, isolated segments within the network to limit lateral movement of attackers.

Answer: D

Explanation: Micro-segmentation involves creating smaller, isolated segments within a network to restrict lateral movement by attackers, thereby enhancing security and minimizing risks.

**Question: 683**

A security team is reviewing their traditional data protection strategies and wants to enhance their defenses against increasingly sophisticated cyber threats. Which approach should they adopt to address the limitations of traditional solutions?

A. Increase reliance on perimeter defenses
B. Limit security measures to endpoint protection
C. Transition to a zero-trust security model
D. Focus exclusively on employee training

Answer: C

Explanation: Transitioning to a zero-trust security model ensures that no user or device is trusted by default, requiring continuous verification and enhancing defenses against sophisticated threats.

**Question: 684**

After a series of breaches, a company decides to implement a threat intelligence program to enhance its cybersecurity posture. Which of the following actions

would be the most beneficial in developing this program?

A. Investing solely in endpoint protection
B. Gathering and analyzing data about emerging threats and vulnerabilities
C. Focusing exclusively on compliance requirements
D. Relying on user-reported incidents only

Answer: B

Explanation: Gathering and analyzing data about emerging threats and vulnerabilities is crucial for an effective threat intelligence program, enabling the organization to proactively address potential risks and improve its security measures.

**Question: 685**

In terms of data security within cloud environments, which Prisma Cloud feature specifically addresses the need for protecting sensitive data and preventing data breaches?

A. Network segmentation.
B. Basic firewall rules.
C. Data Loss Prevention (DLP) capabilities.
D. Static IP whitelisting.

Answer: C

Explanation: Data Loss Prevention (DLP) capabilities in Prisma Cloud focus on protecting sensitive data and preventing data breaches by monitoring and controlling data access and usage across cloud environments.

**Question: 686**

When considering the implementation of a secure network architecture, how does the concept of segmentation enhance both security and performance, particularly regarding the isolation of sensitive systems and the management of network traffic?

A. Segmentation enhances security by isolating sensitive systems from general network traffic, improving performance through reduced congestion and better traffic management.
B. Segmentation reduces overall network performance by introducing complexity in communication paths.
C. Segmentation has no effect on security and is primarily used for performance optimization.
D. The implementation of segmentation complicates security management without providing significant benefits.

Answer: A

Explanation: Segmentation enhances security by isolating sensitive systems from general network traffic, while also improving performance by reducing congestion and enabling better traffic management.

**Question: 687**

During a routine security audit, an organization discovers that their network devices have not been updated with the latest firmware versions, exposing them to vulnerabilities. What is the most effective way to address this issue?

A. Replace all outdated devices with new ones
B. Schedule regular firmware updates and patches
C. Rely on vendor notifications for updates
D. Conduct an audit of all network devices annually

Answer: B

Explanation: Scheduling regular firmware updates and patches ensures that network devices are protected against known vulnerabilities, significantly improving the overall security posture.

**Question: 688**

In a network utilizing IPv6, which of the following addressing features significantly enhances security by allowing the inclusion of authentication information directly in the address?

A. IPv6 extension headers
B. Link-local addressing
C. Unique local addresses
D. Stateless address autoconfiguration

Answer: A

Explanation: IPv6 extension headers can include security-related information, such as authentication and encryption parameters, directly enhancing the security of packets transmitted in an IPv6 network.

**Question: 689**

An enterprise is deploying a next-generation firewall in a hybrid cloud environment. What is the most critical feature the organization should ensure is enabled to provide comprehensive security across both on-premises and cloud environments?

A. Integrated threat intelligence and real-time analysis
B. Basic packet filtering
C. Manual policy configuration for each environment
D. Static IP whitelisting

Answer: A

Explanation: Integrated threat intelligence and real-time analysis provide comprehensive security by enabling the firewall to adapt to threats across both on-premises and cloud environments, improving overall security posture.

**Question: 690**

During a security assessment, a company discovers that its web applications are vulnerable to SQL injection attacks. An attacker could exploit this vulnerability to manipulate database queries. Which of the following actions should the company prioritize to mitigate this risk effectively?

A. Implement stronger password policies
B. Use prepared statements and parameterized queries
C. Conduct regular employee training on phishing
D. Increase firewall rules

Answer: B

Explanation: Using prepared statements and parameterized queries is a strong mitigation strategy against SQL injection attacks, as it ensures that user input is treated as data, not executable code, preventing unauthorized database manipulation.

**Question: 691**

In the context of cybersecurity, what does the term "phishing" refer to?
A. A method of attempting to acquire sensitive information by masquerading as a trustworthy entity in electronic communication.
B. The process of training employees on security best practices.
C. The use of firewalls to block malicious traffic.
D. A technique for encrypting data in transit.

Answer: A

Explanation: Phishing is a cyber attack strategy that seeks to acquire sensitive information by pretending to be a trustworthy entity in electronic communications, often leading to data breaches.

**Question: 692**

Which of the following describes a significant benefit of deploying a Next-Generation Firewall (NGFW) in conjunction with endpoint security solutions?

A. It provides a single point of failure in the network.
B. It offers integrated threat intelligence and visibility across the network and endpoints.
C. It eliminates the need for any endpoint security measures.

D. It simplifies user access controls.

Answer: B

Explanation: NGFWs enhance endpoint security by providing integrated threat intelligence and visibility, enabling organizations to detect and respond to threats that span both network and endpoint environments.

**Question: 693**

In the context of advanced persistent threats, what is the importance of establishing "reconnaissance" as a phase in the attack lifecycle, particularly regarding the intelligence-gathering activities that inform subsequent phases of the attack?

A. Reconnaissance is irrelevant in executing successful attacks.
B. Reconnaissance enables attackers to gather critical information about the target, facilitating tailored attacks.
C. Reconnaissance is solely focused on exploiting technical vulnerabilities.
D. Reconnaissance is limited to identifying physical access points to facilities.

Answer: B

Explanation: Establishing "reconnaissance" as a phase in the attack lifecycle is crucial, as it allows attackers to gather critical information about their target, enabling them to conduct tailored and effective attacks in subsequent phases.

# KILLEXAMS.COM

*Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:*


***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*