PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Certified Cybersecurity Associate

Palo Alto Networks PCCSA

Version Demo

Total Demo Questions: 9

Total Premium Questions: 99

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Palo Alto Networks Cybersecurity Portfolio	8
Topic 2, Cybersecurity Fundamentals	53
Topic 3, Network Security	26
Topic 4, Cloud Security	10
Topic 5, Security Operations	2
Total	99

QUESTION NO: 1

Which two remote access methods are secure because they encrypt traffic? (Choose two.)

A. IPsec-AH

B. SSH

C. VPN

D. Telnet

E. rlogin

ANSWER: B C

Explanation:

SSH and VPN are secure remote-access methods because each provides encryption for data transmitted across an untrusted network. SSH establishes an encrypted connection between a client and a remote host, protecting interactive administrative sessions and other supported functions, such as secure command execution and file transfer. In Palo Alto Networks environments, SSH is commonly used for encrypted command-line access to firewall management interfaces rather than exposing administrative credentials and commands in cleartext.

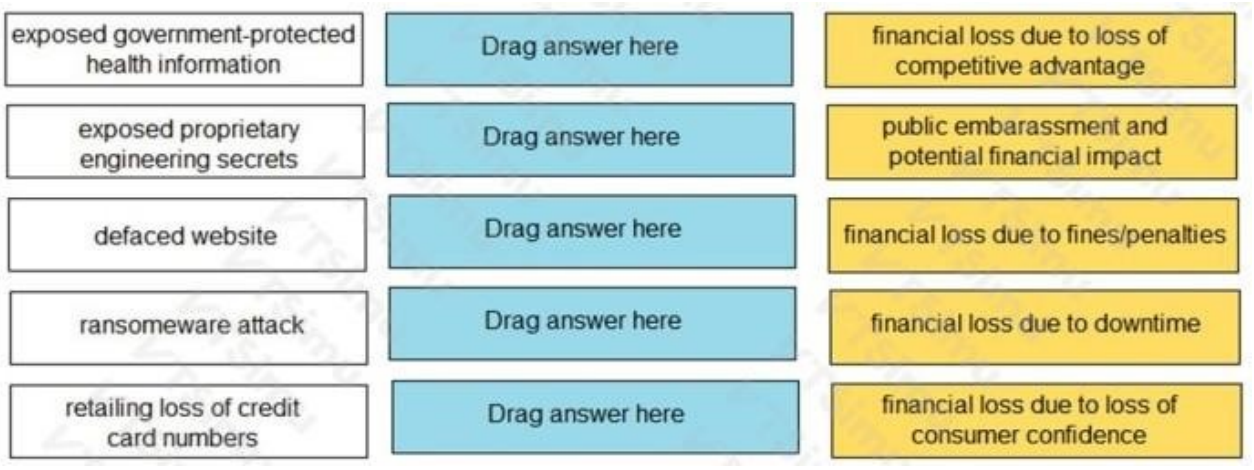
VPN provides an encrypted tunnel between remote users or networks and protected resources. A remote-access VPN allows an individual user to connect securely to an organization's network, while site-to-site VPNs protect traffic between networks. Palo Alto Networks firewalls support IPsec VPNs, which use encryption algorithms to preserve the confidentiality of traffic as it traverses public or otherwise untrusted infrastructure. Encryption is a core VPN security property, enabling users to access internal services without sending application data in readable form over the Internet. Palo Alto Networks documentation describes secure management access and VPN capabilities at Manage Firewall Administrators and IPSec VPN.

QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

Match each type of breach to its consequence.

Select and Place:



ANSWER:

Explanation:

Breaches involving government-protected health information can trigger regulatory enforcement, breach-notification obligations, and monetary penalties because protected health data is subject to strict legal and privacy requirements. In the United States, the Department of Health and Human Services explains that the HIPAA Rules establish protections for individually identifiable health information and that violations can result in civil monetary penalties. See the HHS HIPAA rules overview and the HHS enforcement overview.

Engineering secrets represent intellectual property and confidential business knowledge. When exposed, competitors may gain insight that reduces the organization's differentiation and weakens its competitive position, producing financial loss tied to lost competitive advantage. A website defacement is externally visible, so its immediate consequence is reputational harm and public embarrassment; restoration, incident response, lost sales, and customer concerns can also create a financial impact.

Ransomware commonly encrypts systems or otherwise prevents access to business resources. Even when data recovery is possible, interrupted operations can stop production, delay services, and require remediation work. This makes downtime a direct and central financial consequence. The CISA StopRansomware guidance describes ransomware as a threat that can impact the availability of systems and data.

A loss of retail credit-card numbers affects customers directly and can damage their trust in the retailer's ability to protect payment information. That erosion of trust can reduce future purchasing and loyalty, creating financial loss through reduced consumer confidence. These mappings connect each incident's primary affected asset or operational impact to the most natural business consequence.

QUESTION NO: 3

Which type of cloud computing deployment makes resources exclusively available to members of a single organization?

A. local

B. private

C. hybrid

D. public

ANSWER: B

Explanation:

Private is correct because a private cloud is provisioned for exclusive use by one organization. Its computing resources, such as servers, storage, networking, and cloud-management capabilities, are dedicated to that organization rather than shared broadly among unrelated customers. The organization may own and operate the infrastructure itself, or a third party may manage it; it may also be located on premises or hosted externally. The defining characteristic is exclusive organizational use and the greater control this model provides over security policies, governance, compliance requirements, and resource configuration. This makes private cloud deployment particularly appropriate when an organization has strict regulatory, data-residency, customization, or isolation needs while still wanting cloud-style elasticity and self-service

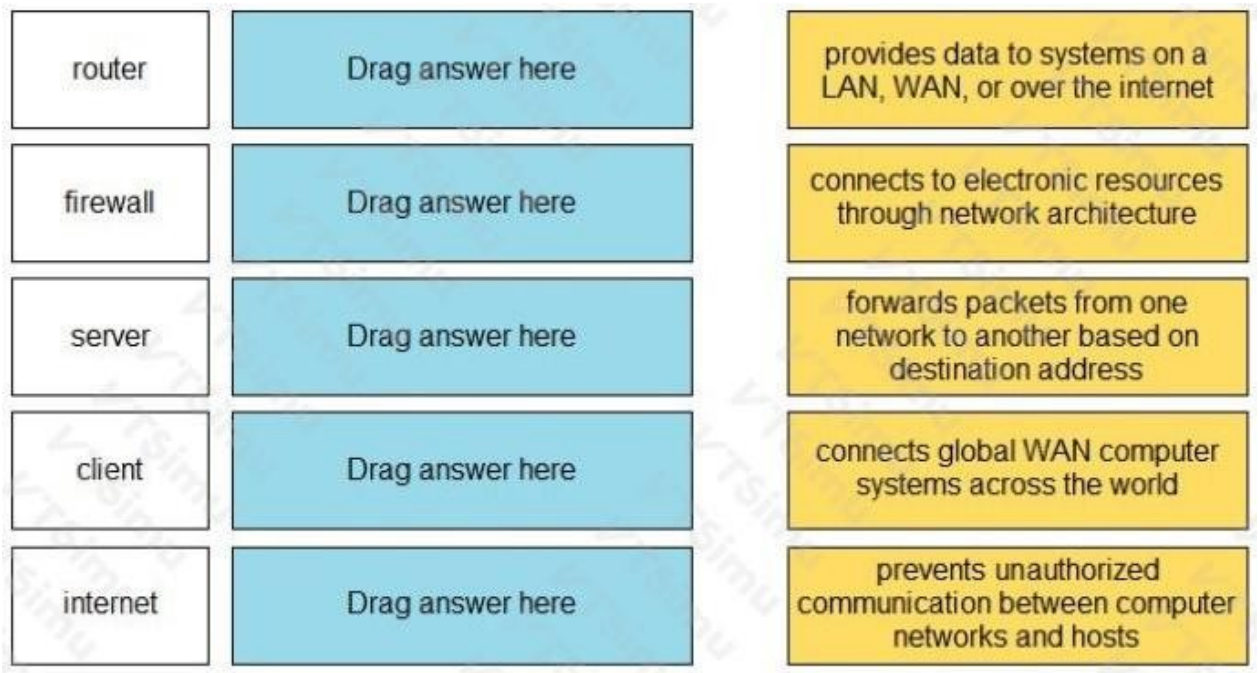
capabilities. The National Institute of Standards and Technology defines a private cloud as cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers or business units. Palo Alto Networks similarly describes private cloud as a cloud environment dedicated to a single organization. See the NIST definition of cloud computing and Palo Alto Networks' private cloud overview.

QUESTION NO: 4 - (DRAG DROP)

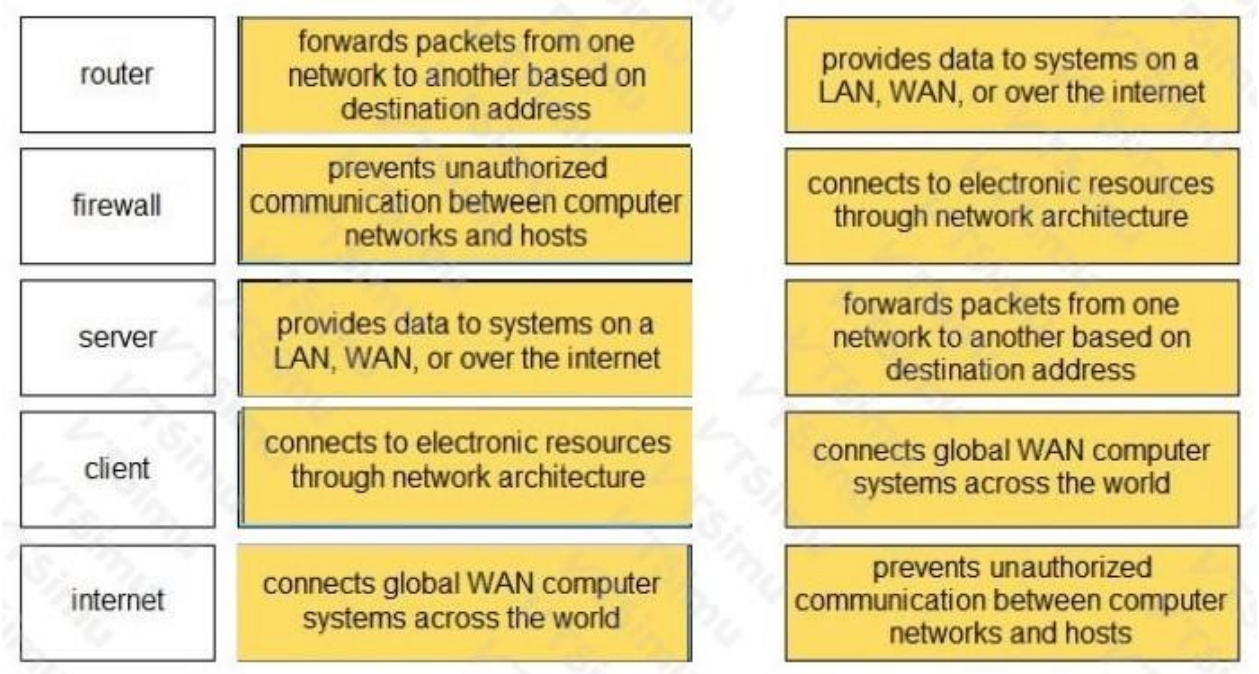
DRAG DROP

Match the network infrastructure item with its corresponding description.

Select and Place:



ANSWER:



Explanation:

The completed matching is correct because each description identifies the core role of that network infrastructure component. A router operates at the network layer and makes forwarding decisions so that packets can travel from one network to another using destination addressing information. Palo Alto Networks describes routing as forwarding traffic between networks, and the foundational routing behavior is also defined by the IETF in Requirements for IP Version 4 Routers.

A firewall enforces security policy between hosts and networks. Its purpose is to control communications and prevent traffic that is not authorized by the organization's policy. This matches Palo Alto Networks' description of a firewall as a security device that monitors and controls network traffic; see the Palo Alto Networks firewall overview.

A server provides data, applications, or other services to systems that request them, whether those systems are connected locally on a LAN, remotely through a WAN, or through the internet. A client is the endpoint or software that connects through the network architecture to access those electronic resources. This client-server relationship is the standard model for delivering shared resources and services over networks.

The internet is the worldwide interconnection of networks and WAN-connected computer systems. It enables systems across geographic regions to exchange information using common protocols, especially the Internet Protocol suite. The Internet Society's history of the Internet explains how this global network developed as interconnected networks using shared standards. Together, the mappings accurately distinguish packet forwarding, security enforcement, service delivery, resource consumption, and global network interconnection.

QUESTION NO: 5

Which type of attack floods a target with TCP SYN requests?

A. route table poisoning

B. reconnaissance

C. denial-of-service

D. IP spoofing

ANSWER: C

Explanation:

A TCP SYN flood is a denial-of-service attack. It abuses the TCP three-way handshake by sending a very large number of SYN packets to a target. For each received SYN, the target typically allocates resources and responds with a SYN-ACK while awaiting the final ACK that would complete the connection. When requests arrive faster than they can be completed or cleared, the target's half-open connection queue and related resources can become exhausted. Legitimate clients may then be unable to establish new TCP sessions, which is the intended availability impact of a denial-of-service attack.

The source addresses in SYN flood traffic are often forged, but the defining attack category in this question is denial of service: the purpose is to overwhelm connection-handling capacity and disrupt access to the service. Palo Alto Networks threat-prevention guidance identifies TCP SYN flood protection as a mechanism for detecting and mitigating this type of resource-exhaustion attack. See the Palo Alto Networks documentation on Zone Protection and DoS Protection and CISA's overview of denial-of-service attacks.

QUESTION NO: 6

Which two principles are associated with a Zero Trust security strategy? (Choose two.)

A. verify explicitly

B. trust all internal devices by default

C. use least-privileged access

D. allow unrestricted lateral movement

ANSWER: A C

Explanation:

Verify explicitly and **use least-privileged access** are core Zero Trust principles. Explicit verification requires organizations to evaluate relevant signals, such as user identity, device posture, location, and requested resource, before granting access. Trust is not granted merely because a device is connected to an internal network.

Least-privileged access limits users and systems to only the resources and permissions needed for authorized tasks. This reduces the potential impact of compromised credentials, malicious insiders, and lateral movement. Zero Trust replaces implicit trust based on network location with continuous, context-aware access decisions. See Palo Alto Networks' Zero Trust overview and NIST SP 800-207.

QUESTION NO: 7

Which component of a digital certificate provides authentication of the certificate's issuer?

A. digital signature

B. certificate revocation list

C. issuer's private key

D. certificate's expiration date

ANSWER: A

Explanation:

The digital signature provides authentication of the certificate's issuer. When a certificate authority issues a certificate, it calculates a cryptographic signature over the certificate's encoded data using the authority's private key. A client or security device that receives the certificate uses the issuer's trusted public key to verify that signature. Successful verification demonstrates that the certificate data was signed by the holder of the corresponding issuer private key and that the signed certificate contents have not been modified since signing. This cryptographic verification establishes the issuer's authenticity within the trust chain, provided that the issuer certificate or trust anchor is trusted by the verifying system.

In X.509 certificates, the signature algorithm and signature value are defined certificate fields, and relying parties validate the certificate signature during path validation. Palo Alto Networks firewalls similarly rely on trusted certificate authority certificates to validate certificate chains when performing functions such as SSL/TLS decryption and server certificate verification. See RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile and Palo Alto Networks SSL Forward Proxy Decryption documentation.

QUESTION NO: 8

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

A. tolerated

B. certified

C. sanctioned

D. unsanctioned

ANSWER: A C

Explanation:

"sanctioned" and "tolerated" are the SaaS application categories that an IT department permits for use. Sanctioned applications have been formally reviewed and approved by the organization. They are typically selected because they meet

established requirements for business value, security controls, compliance, identity integration, and data handling. This formal approval lets IT define how the service should be used and apply appropriate governance.

Tolerated applications are also allowed, but they have a different governance status. The organization recognizes that users need or use these services and permits access, even though the applications may not have completed the same level of formal approval, procurement, or security assessment as sanctioned services. Identifying tolerated services enables security teams to maintain visibility, assess risk, and apply policies that protect organizational data while supporting practical business needs.

Palo Alto Networks describes SaaS security as requiring visibility and control over the cloud applications employees use, including distinguishing approved and managed usage from other application activity. See Palo Alto Networks: SaaS Security and Palo Alto Networks: SaaS Security Solutions.

QUESTION NO: 9

Which capability is required for a next-generation firewall to protect your network against malware threats?

A. can access/read Windows and Linux file systems

B. can scan all endpoint devices

C. can interpret file permissions

D. can perform SSL decryption

ANSWER: D

Explanation:

To protect a network effectively against malware, a next-generation firewall must be able to perform SSL decryption. A significant amount of modern web, application, and command-and-control traffic is encrypted with SSL/TLS. Although encryption protects confidentiality in transit, it also prevents a firewall from viewing the actual file contents, URLs, and payloads needed for security inspection. SSL decryption allows the firewall to decrypt supported traffic, apply its security policies and threat-prevention inspection to the clear-text content, and then re-encrypt the traffic before forwarding it. This enables Palo Alto Networks security services, including antivirus and advanced threat prevention capabilities, to identify and block malware delivered over encrypted connections. Decryption policy should be deployed thoughtfully, with exclusions for traffic that should not be decrypted due to privacy, legal, regulatory, or technical requirements. Palo Alto Networks documents that decrypted traffic can be inspected by security policy and security profiles, making SSL decryption an essential visibility capability when malware may be concealed in encrypted sessions. See the Palo Alto Networks Decryption documentation and the Virus and WildFire Analysis documentation.