PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Cybersecurity

Palo Alto Networks Practitioner

Version Demo

Total Demo Questions: 25

Total Premium Questions: 250

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cybersecurity Fundamentals	70
Topic 2, Network Security	65
Topic 3, Cloud Security	56
Topic 4, Security Operations	58
Topic 5, Mix Questions	1
Total	250

QUESTION NO: 1

Layer 4 of the TCP/IP Model corresponds to which three Layer(s) of the OSI Model? (Choose three.)

A. Network

B. Application

C. Session

D. Transport

E. Presentation

ANSWER: B C E

Explanation:

In the commonly taught four-layer TCP/IP model numbered from the lowest layer upward, Layer 4 is the Application layer. This TCP/IP layer combines the functions that the seven-layer OSI model separates into the Application, Presentation, and Session layers. Application-layer protocols provide network services directly to user applications, while the associated OSI functions include establishing and managing application dialogs, representing data in an interoperable format, and supporting services such as encoding, encryption, and compression. For example, protocols such as HTTP, DNS, SMTP, and SSH operate at the TCP/IP Application layer even though their end-to-end communication may involve OSI session and presentation functions. Palo Alto Networks training material commonly uses the TCP/IP model to describe where network protocols and security controls operate; understanding that its upper Application layer encompasses these three OSI layers helps analysts identify protocol behavior and apply appropriate policy inspection. The Transport layer is a separate TCP/IP layer and maps directly to the OSI Transport layer, rather than being part of the three-layer grouping asked for here. See Palo Alto Networks' TCP/IP model overview and its OSI model overview.

QUESTION NO: 2

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

A. SaaS

B. PaaS

C. On-premises

D. IaaS

ANSWER: A B

Explanation:

SaaS and **PaaS** are the cloud service models in which the vendor manages vulnerability remediation and patching for the underlying operating system. Under the shared-responsibility model, SaaS provides a complete, ready-to-use application. Because the provider operates the application and the platform on which it runs, the provider maintains the underlying infrastructure, operating system, and associated platform components, including applying security patches.

With PaaS, the provider supplies and operates the managed application platform, including the servers, networking, storage, runtime environment, and underlying operating system. Customers focus on the applications and data they deploy to that platform, while the vendor is responsible for maintaining and securing the managed OS layer. This allocation lets development teams build and deploy applications without administering operating-system updates directly. Responsibility boundaries can vary slightly by specific service and contract, but the standard SaaS/PaaS/IaaS shared-responsibility model assigns underlying OS patch management to the provider for SaaS and PaaS. See Palo Alto Networks' cloud security overview and the NIST cloud-computing definition for service-model context.

QUESTION NO: 3

Which two capabilities are appropriate for API-based SaaS Security protection? (Choose two.)

A. Scanning data stored in connected SaaS applications

B. Identifying sensitive data that has been shared too broadly

C. Blocking a user upload before it reaches a SaaS application

D. Preventing local malware execution on an endpoint

ANSWER: A B

Explanation:

Scanning data stored in connected SaaS applications and **identifying sensitive data that has been shared too broadly** are correct. API-based SaaS Security connects to supported SaaS applications to inspect data at rest, identify sensitive content, and detect exposure caused by risky sharing settings or permissions.

Inline inspection and immediate blocking of a user upload require traffic to pass through an inline enforcement point, such as a secure web gateway or an inline CASB capability. API-based scanning also does not replace endpoint protection on managed devices.

QUESTION NO: 4

Which item accurately describes a security weakness that is caused by implementing a “ports first” data security solution in a traditional data center?

A. You may have to use port numbers greater than 1024 for your business-critical applications.

B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.

C. You may not be able to assign the correct port to your business-critical applications.

D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

ANSWER: B

Explanation:

You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter. This accurately captures the fundamental exposure created by a ports-first security model: the policy decision is primarily based on transport-layer ports rather than the actual application, its function, and the user or device initiating it. Modern applications frequently use dynamic ports, port hopping, encrypted traffic, and nonstandard ports. To maintain business connectivity under a port-based model, administrators can be forced to allow broad port ranges or additional services. Each permitted port expands the pathways that can reach internal systems and can allow unauthorized or malicious traffic that is using an approved port. Palo Alto Networks promotes an application-first approach through App-ID, which identifies applications regardless of port, protocol, encryption, or evasive technique. Security policy can then allow only the specific, sanctioned applications required for the business, reducing unnecessary exposure while still enabling legitimate services. This principle supports least-privilege network access: permit only the known application traffic that is needed, rather than trusting traffic merely because it uses an allowed port. See Palo Alto Networks’ Application-Based Policy documentation and its overview of App-ID.

QUESTION NO: 5

Which two outcomes can User-ID provide when it is integrated with a directory service? (Choose two.)

A. Applying Security policy to directory users and groups

B. Assigning IP addresses to authenticated endpoints

C. Associating an IP address with an authenticated username

D. Decrypting SSL/TLS traffic for identified users

ANSWER: A C

Explanation:

Applying Security policy to directory users and groups and **associating an IP address with an authenticated username** are correct. User-ID maps user identities to IP addresses and can obtain group membership from a directory service. This enables administrators to create and enforce policy based on users and groups rather than relying only on source IP addresses.

User-ID does not replace directory-service authentication, assign IP addresses to endpoints, or decrypt traffic. It provides identity context that can be used by Security policy and displayed in logs.

QUESTION NO: 6

Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

A. cybercriminals

B. state-affiliated groups

C. hacktivists

D. cyberterrorists

ANSWER: D

Explanation:

cyberterrorists is correct. Cyberterrorism is associated with the use of digital technologies and the internet in support of ideological, political, or religious objectives, particularly where the intended effect is to intimidate or coerce a population and create fear or panic. The internet can serve several operational and propaganda purposes for such groups: distributing ideological messaging, recruiting and radicalizing supporters, providing training materials or instructions, coordinating activity, and amplifying the psychological impact of threats or attacks through rapid, broad dissemination. The defining element in this attacker profile is not simply unauthorized technical activity; it is the objective of advancing an ideology through intimidation and fear. Palo Alto Networks' cybersecurity education materials categorize attackers by their motivations and describe cyberterrorists as actors driven by ideological aims who seek to cause fear and disruption. This profile also aligns with the broader understanding of terrorism as violence or threats intended to intimidate or coerce civilians or influence policy. For additional background, see Palo Alto Networks' Cyberterrorism overview and the U.S. Cybersecurity and Infrastructure Security Agency's cyber threats guidance.

QUESTION NO: 7

An organization deploys business applications on virtual machines in an IaaS environment. Which two responsibilities commonly remain with the organization under the shared-responsibility model? (Choose two.)

A. Patching and hardening guest operating systems

B. Configuring application access controls and protecting application data

C. Replacing failed physical servers in the provider data center

D. Maintaining the provider's physical building security systems

ANSWER: A B

Explanation:

In an IaaS model, the cloud provider manages the underlying physical facilities, hardware, and virtualization infrastructure. The customer remains responsible for securing the virtual machines and the applications and data it deploys. This includes maintaining guest operating systems and configuring access controls appropriate to the workload.

The provider, rather than the customer, is generally responsible for replacing failed physical servers and maintaining the physical data-center infrastructure. Responsibility details can vary by service, but these are the standard IaaS boundaries.

QUESTION NO: 8

A native hypervisor runs:

A. with extreme demands on network throughput

B. only on certain platforms

C. within an operating system's environment

D. directly on the host computer's hardware

ANSWER: D

Explanation:

Directly on the host computer's hardware is correct because a native hypervisor, also called a Type 1 or bare-metal hypervisor, is installed directly on the physical server rather than being installed as an application on a conventional host operating system. It provides the virtualization layer that allocates physical compute, memory, storage, and networking resources to virtual machines. Because it operates at this foundational layer, it can manage guest operating systems while maintaining isolation between workloads and efficiently controlling access to the underlying hardware. This architecture is widely used for enterprise data centers and cloud environments, where centrally managed virtualization and workload separation are essential. Palo Alto Networks' cloud-security materials distinguish virtualized environments and their hypervisor layer as core infrastructure requiring appropriate visibility and protection. For a general technical definition of Type 1 hypervisors, see VMware: What is a Hypervisor?. The National Institute of Standards and Technology also describes the hypervisor as the software layer that enables virtual machines to share underlying hardware resources in its SP 800-125 guidance on security for virtualization technologies.

QUESTION NO: 9

What is the recommended method for collecting security logs from multiple endpoints?

A. Leverage an EDR solution to request the logs from endpoints.

B. Connect to the endpoints remotely and download the logs.

C. Configure endpoints to forward logs to a SIEM.

D. Build a script that pulls down the logs from all endpoints.

ANSWER: C

Explanation:

Configure endpoints to forward logs to a SIEM. A security information and event management platform provides a centralized, scalable destination for telemetry from many endpoint systems. Endpoint log forwarding enables security teams to collect, normalize, correlate, search, and retain event data without requiring an analyst to manually connect to individual devices during an investigation. This approach supports continuous visibility and allows detections to combine endpoint events with identity, network, cloud, and other security data sources. It also improves operational consistency because collection and retention policies can be managed centrally, while alerts can be generated when correlated activity indicates potential malicious behavior. In Palo Alto Networks environments, Cortex XSIAM and Cortex XDR can ingest endpoint telemetry and broader log sources to support investigation, analytics, and response workflows. A SIEM-oriented forwarding

architecture is therefore the recommended general practice for security-log collection across multiple endpoints. Palo Alto Networks describes centralized logging and analytics capabilities in its Cortex XSIAM documentation, and NIST explains the role of centralized log management in SP 800-92: Guide to Computer Security Log Management.

QUESTION NO: 10

Which two statements apply to the SSL/TLS protocol? (Choose two.)

A. It contains password characters that users enter to access encrypted data.

B. It is a method used to encrypt data and authenticate web-based communication.

C. It ensures the data that is transferred between a client and a server remains private.

D. It provides administrator privileges to manage and control the access of network resources.

ANSWER: B C

Explanation:

SSL/TLS is a cryptographic protocol suite used to protect communications between endpoints, commonly a web browser or application client and a web server. It is used to encrypt data in transit and to authenticate the communicating server through digital certificates; in some deployments, TLS can also authenticate the client. During the TLS handshake, the endpoints negotiate cryptographic parameters, validate certificate information, and establish session keys that protect the subsequent application traffic.

By encrypting the connection, TLS provides confidentiality for data transferred between a client and server, helping prevent unauthorized parties that can observe network traffic from reading the contents. TLS also provides integrity protection, enabling the endpoints to detect unauthorized modification of protected traffic while it is in transit. These protections are fundamental to HTTPS, which uses HTTP over TLS to secure web-based communication. Palo Alto Networks firewalls can inspect SSL/TLS traffic when configured for decryption, allowing security policy enforcement and threat inspection while maintaining appropriate certificate and privacy practices. See RFC 8446, The Transport Layer Security Protocol Version 1.3 and Palo Alto Networks' SSL Forward Proxy Decryption documentation.

QUESTION NO: 11

Which SOAR feature coordinates across technologies, security teams, and external users for centralized data visibility and action?

A. Case management

B. Integrations

C. Ticketing system

D. Playbooks

ANSWER: D

Explanation:

Playbooks are the SOAR feature that defines and executes repeatable workflows for investigating, enriching, containing, and responding to security events. A playbook can connect the operational steps that need to occur across security technologies, analysts and other teams, and external parties. For example, it can retrieve context from threat-intelligence sources, query endpoint or network controls, notify an incident owner, request an approval, open or update a case, and perform a containment action. This coordinated workflow gives responders a centralized operational view of the incident while ensuring actions occur in a defined, consistent sequence. Palo Alto Networks describes SOAR as combining orchestration, automation, and response capabilities to help security teams standardize and accelerate incident handling. Within that model, playbooks provide the workflow logic that coordinates integrated tools and people, reducing repetitive manual work

and making response processes more consistent and auditable. See Palo Alto Networks' overview of security orchestration, automation, and response (SOAR) and its Cortex XSOAR documentation on playbooks.

QUESTION NO: 12

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

A. People

B. Accessibility

C. Processes

D. Understanding

E. Business

ANSWER: A C E

Explanation:

People, Processes, and Business complete the six SecOps elements: business, people, interfaces, visibility, technology, and processes. The business element establishes the organization's risk priorities, intended outcomes, and operational objectives. Those goals provide the context for security decisions and for measuring whether SecOps is delivering meaningful results. People are the analysts, responders, engineers, and other stakeholders who perform and coordinate security work; successful operations require clearly defined responsibilities and collaboration across these roles. Processes are the repeatable operational workflows used to detect, investigate, prioritize, respond to, and learn from security events. Together, these elements ensure that the tools and data used by a security team support an intentional operating model rather than functioning as isolated technical capabilities. Palo Alto Networks describes modern security operations as an integrated practice that combines people, processes, and technology to improve prevention, detection, investigation, and response. This framing also emphasizes aligning the SOC's work to organizational objectives and continuously improving operational outcomes. See Palo Alto Networks' overview of security operations centers and its security operations resources.

QUESTION NO: 13

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

Explanation:

connectors and interfaces are required because they establish the operational path that moves security telemetry from a system of interest into the SIEM's data lake in a usable form. A connector integrates with a particular source—such as a firewall, endpoint platform, cloud service, identity provider, or application—and collects its events through methods such as APIs, agents, syslog, or cloud messaging services. The interface provides the communication and ingestion path through which that collected telemetry is delivered to the SIEM. During ingestion, the SIEM can parse, normalize, enrich, and map the source records into a common schema, allowing the data lake to store it consistently and enabling searches, detections, investigations, and correlation across sources. In Palo Alto Networks Cortex XSIAM, integrations and collectors support the ingestion of third-party and Palo Alto Networks data, while parsers convert raw logs into fields that analytics and detection content can use. Thus, connectors and interfaces are the necessary integration components for a translated end-to-end data

flow rather than merely underlying hosting resources. See the Cortex XSIAM data-ingestion documentation and the Cortex XSIAM parser documentation.

QUESTION NO: 14

What is a purpose of workload security on a Cloud Native Security Platform (CNSP)?

A. To provide automation for application creation in the cloud

B. To secure serverless functions across the application

C. To secure public cloud infrastructures only

D. To provide comprehensive logging of potential threat vectors

ANSWER: B

Explanation:

To secure serverless functions across the application is correct because workload security protects the compute workloads that run cloud-native applications, including hosts, containers, Kubernetes workloads, and serverless functions. Serverless code remains a workload even though the cloud provider manages the underlying servers; it still requires visibility into vulnerabilities, insecure configurations, excessive permissions, and runtime activity. In Palo Alto Networks Prisma Cloud, workload protection is designed to provide protection across the application lifecycle, combining preventative security controls with runtime defense for cloud workloads. For serverless deployments, this includes assessing function code and configuration, identifying risks in dependencies and permissions, and monitoring runtime behavior to help identify threats affecting the function and the application it supports. Securing these functions is therefore a direct purpose of workload security, rather than simply an operational cloud-automation task. Palo Alto Networks describes its cloud workload protection capabilities at Prisma Cloud Workload Protection. Additional details on protecting serverless workloads are available in the Prisma Cloud Compute documentation.

QUESTION NO: 15

Which of the Cloud-Delivered Security Services (CDSS) will detect zero-day malware by using inline cloud machine learning (ML) and sandboxing?

A. DNS security

B. Advanced WildFire

C. IoT security

D. Advanced Threat Prevention

ANSWER: B

Explanation:

Advanced WildFire is the Cloud-Delivered Security Service designed to identify and prevent unknown and zero-day malware through a combination of inline cloud machine learning and cloud-based sandbox analysis. When the firewall encounters files or other content that require deeper inspection, Advanced WildFire applies machine-learning models to rapidly classify malicious characteristics and can submit unknown samples for advanced analysis in the WildFire cloud sandbox. This layered approach enables detection of previously unseen threats rather than relying only on existing antivirus signatures. Palo Alto Networks describes Advanced WildFire as providing inline AI-driven analysis for real-time prevention alongside cloud sandboxing for comprehensive malware detection. The service continuously produces threat intelligence from analyzed samples, allowing protections to be distributed quickly across protected environments. This makes Advanced WildFire the appropriate service when the requirement specifically combines zero-day malware detection, inline cloud ML, and sandboxing. See the Advanced WildFire overview and Palo Alto Networks' Advanced WildFire product page for details.

QUESTION NO: 16

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

Explanation:

SOAR is correct because Security Orchestration, Automation, and Response platforms are specifically designed to operationalize incident-response workflows using standardized playbooks. A SOAR platform ingests alerts, context, and telemetry from security products and other data sources, then coordinates actions across those tools. Its playbooks can automate repeatable steps such as enriching an alert with threat intelligence, opening and updating a case, gathering endpoint or network evidence, notifying responders, and—when policy permits—initiating containment actions. This orchestration reduces the time required to investigate and respond while making handling more consistent and less dependent on manual, ad hoc processes. Palo Alto Networks Cortex XSOAR is an example of this technology: it provides playbooks for automating and orchestrating security operations and incident response across integrated products. The term therefore directly matches a system that executes automated playbooks based on inputs from security technologies and data flows. See Palo Alto Networks' Cortex XSOAR overview and its SOAR definition.

QUESTION NO: 17

What are two advantages of security orchestration, automation, and response (SOAR)? (Choose two.)

A. Completely isolated system

B. Scripting of manual tasks

C. Consistent incident handling

D. Long-term retention of logs

ANSWER: B C

Explanation:

Scripting of manual tasks and **Consistent incident handling** are key advantages of SOAR. SOAR platforms use integrations, automation, scripts, and playbooks to perform repetitive investigation and response activities that analysts might otherwise complete manually. For example, a playbook can enrich an alert with threat-intelligence data, collect relevant endpoint or network context, create a case, and initiate approved containment actions. This reduces time spent on routine operational steps and allows security teams to focus their expertise on higher-value analysis and decisions.

SOAR also improves consistency because documented playbooks provide a repeatable workflow for common incident types. Each alert or incident can be triaged, investigated, escalated, and responded to using the organization's established process. This supports predictable handling, reduces variation between analysts or shifts, and helps teams maintain an auditable response process. Palo Alto Networks Cortex XSOAR describes playbooks as the mechanism for automating and orchestrating security processes, while incident-management capabilities centralize and standardize case handling. See Palo Alto Networks Cortex XSOAR and Automate Tasks in Playbooks.

QUESTION NO: 18

In SecOps, what are two of the components included in the identify stage? (Choose two.)

A. Initial Research

B. Change Control

C. Content Engineering

D. Breach Response

ANSWER: A C

Explanation:

The identify stage establishes the operational and technical foundation for a SecOps program. **Initial Research** is included because the team must first understand the organization's environment, including critical assets, business priorities, likely threats, existing controls, data sources, and the risks that require security monitoring. This discovery work helps define meaningful use cases and ensures that later operational processes are aligned with what the organization needs to protect.

Content Engineering is also part of identification because researched risks and use cases must be translated into usable security content. This includes designing, tuning, validating, and maintaining items such as detection logic, correlation rules, alerts, dashboards, threat indicators, and related workflows. Effective security content gives the operations team a practical way to recognize relevant activity in the telemetry it collects. Together, initial research supplies the context and priorities, while content engineering operationalizes that knowledge into detections and security operations capabilities. Palo Alto Networks positions Cortex products around using integrated data, analytics, and automation to improve detection and investigation operations; see Cortex XSIAM and the Security Operations Center overview.

QUESTION NO: 19

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

A. encryption

B. port scanning

C. DNS tunneling

D. port evasion

ANSWER: B

Explanation:

Port scanning is the correct answer because it is a core reconnaissance and attack-enablement technique used to identify reachable hosts, open ports, listening services, and potentially vulnerable applications. By probing a target for exposed TCP or UDP ports and examining the responses, an attacker can determine which services are available—for example, web servers, remote-access services, databases, or administrative interfaces. The discovered service and version information can then be matched to known weaknesses or used to select an appropriate exploit method. In a security operations context, port-scanning activity is therefore highly relevant because it often precedes attempted exploitation and helps an attacker focus on accessible attack surfaces. Palo Alto Networks NGFW security capabilities, including vulnerability protection and threat prevention, help inspect traffic associated with exploit attempts against vulnerable services and applications. Security teams should use logs and threat-prevention controls to identify suspicious probing and reduce the exposed attack surface by allowing only required services and ports. See Palo Alto Networks' Security Policy documentation and the Vulnerability Protection documentation for information on controlling application access and protecting vulnerable services.

QUESTION NO: 20 - (SIMULATION)

Match each description to a Security Operating Platform key capability.

ANSWER: See the explanation for the answer

Explanation:

Correct matches:

Best-of-breed technologies natively integrated; positive control based on applications, users, and content; open communication, orchestration, and visibility → Reduce the attack surface.
A coordinated platform that considers the full scope of an attack across security controls to quickly identify and block threats → Prevent all known threats, fast.
Automatically create and distribute near-real-time protections for new threats and dynamically update policy so defenses scale with technology rather than people → Detect and prevent new, unknown threats with automation.

QUESTION NO: 21

Which element of the security operations process is concerned with using external functions to help achieve goals?

A. interfaces

B. business

C. technology

D. people

ANSWER: A

Explanation:

interfaces is correct because the Interfaces pillar of the security operations process addresses the external functions, teams, services, and touchpoints a security organization relies on to achieve its operational and business goals. Security operations does not function in isolation: it must interact with stakeholders and supporting functions such as IT operations, network teams, identity teams, legal and compliance groups, managed service providers, threat-intelligence sources, and incident-response partners. Defining these interfaces clarifies how work, information, requests, ownership, and escalation paths move across organizational boundaries. This enables the security team to obtain needed support and coordinate effective action while remaining aligned with its intended outcomes. In Palo Alto Networks' security-operations approach, the six pillars provide a structured way to evaluate whether the operating model has the necessary organizational connections, visibility, capabilities, people, and repeatable execution needed to protect the business. Well-designed interfaces therefore make external collaboration deliberate and dependable rather than informal or ad hoc. For broader context on security operations and the role of coordinated capabilities in a SOC, see Palo Alto Networks' Security Operations Center overview and its Security Operations resources.

QUESTION NO: 22

What are two functions of an active monitoring system? (Choose two.)

A. Preventing specific changes from being affected in the system

B. Determining system health using unaltered system data

C. Detecting micro-services in a default configuration

D. Using probes to establish potential load issues

E. Simulating user transactions to verify service availability and response time

ANSWER: D E

Explanation:

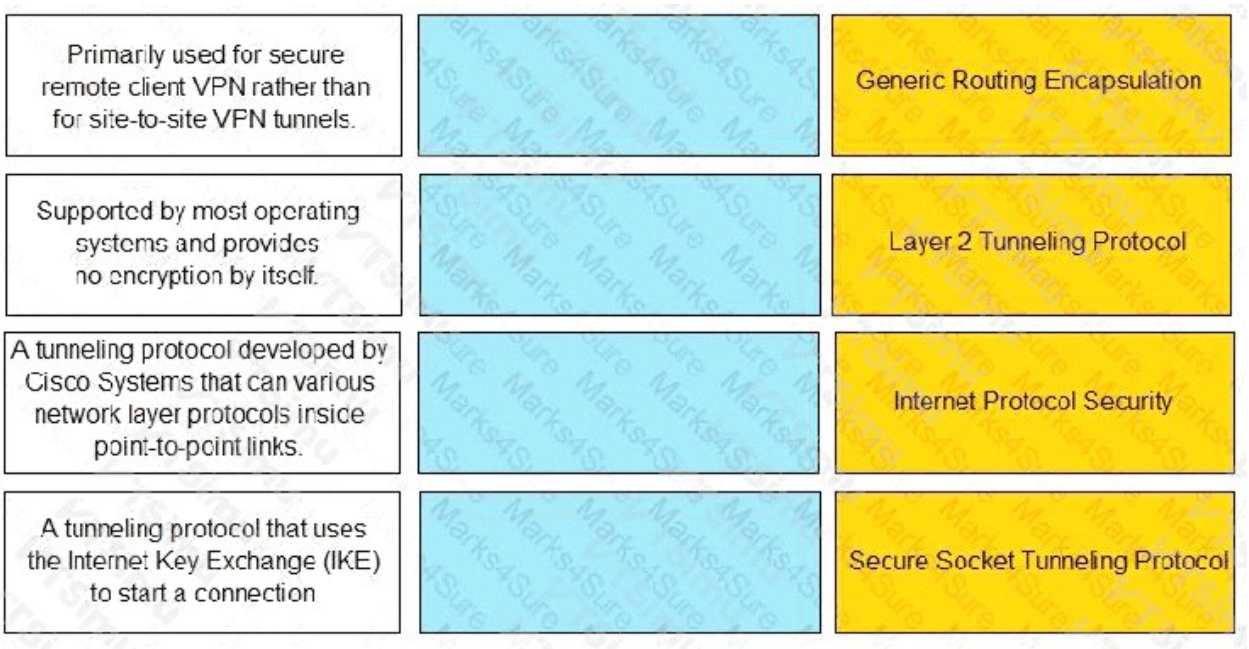
Active monitoring proactively generates or initiates activity against an application, service, or network target rather than waiting for organically produced traffic or telemetry. Using probes to establish potential load issues is therefore an active-

monitoring function: probes can generate controlled requests and collect measurements that help teams identify capacity constraints, latency, and other performance concerns before they have widespread user impact.

Simulating user transactions to verify service availability and response time is also an active-monitoring function. Synthetic tests can repeatedly exercise important workflows—such as reaching a web endpoint, resolving a service, or completing a transaction—from defined locations. The resulting availability and performance data gives operations teams an objective, repeatable way to validate the user experience and detect degradation proactively. Palo Alto Networks ADEM supports synthetic monitoring to test application reachability and performance through scheduled, simulated tests. See the Palo Alto Networks ADEM synthetic monitoring documentation and the PAN-OS monitoring documentation for additional monitoring guidance.

QUESTION NO: 23 - (SIMULATION)

Match the description with the VPN technology.



ANSWER: See the explanation for the answer

Explanation:

Correct matches:

L2TP is commonly paired with IPsec because L2TP supplies tunneling but does not encrypt traffic on its own. IPsec uses IKE for security association negotiation.

QUESTION NO: 24

Which term describes establishment of on-premises software on a cloud-based server?

A. Serverless

B. Dockers

C. Cloud-hosted

D. Kubernetes

ANSWER: C

Explanation:

Cloud-hosted describes deploying or running an application that was traditionally operated on premises on infrastructure hosted by a cloud provider. In this model, the organization moves the application's compute, storage, and networking environment to cloud-based servers, often using virtual machines, while retaining much of the existing application architecture and operational model. This is commonly associated with a "lift-and-shift" migration approach: the workload gains the scalability, availability options, and consumption model of cloud infrastructure without necessarily being redesigned as a cloud-native application. Palo Alto Networks distinguishes cloud-hosted applications and workloads from cloud-native ones when discussing how organizations secure applications across cloud environments. A cloud-hosted workload may therefore require security controls appropriate to its cloud infrastructure while still reflecting the design and dependencies of its original on-premises deployment. See Palo Alto Networks' discussion of cloud security and workload protection at https://www.paloaltonetworks.com/cloud-security and its overview of cloud migration approaches at https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-migration.

QUESTION NO: 25

Which two network resources does a directory service database contain? (Choose two.)

A. Services

B. /etc/shadow files

C. Users

D. Terminal shell types on endpoints

ANSWER: A C

Explanation:

Services and Users are correct because a directory service stores structured identity and resource information that can be searched, managed, and used to control access across a network. User entries typically contain identity attributes such as usernames, group memberships, authentication-related details, and other organizational information. Service-related entries describe network-accessible capabilities or resources, enabling systems and administrators to identify and locate services in the environment. Directory services therefore provide a centralized source of information that supports authentication, authorization, resource discovery, and policy enforcement.

In Palo Alto Networks environments, User-ID uses directory-service information to associate users and groups with IP addresses and to apply Security policy based on identity rather than only network addresses. This identity context is especially important for enforcing least-privilege access and for obtaining meaningful visibility into user activity. Palo Alto Networks documentation describes how User-ID integrates with directory services and uses user and group information in policy decisions: Palo Alto Networks User-ID Overview. For background on directory services and their role in centrally managing users and resources, see Microsoft Active Directory Domain Services overview.