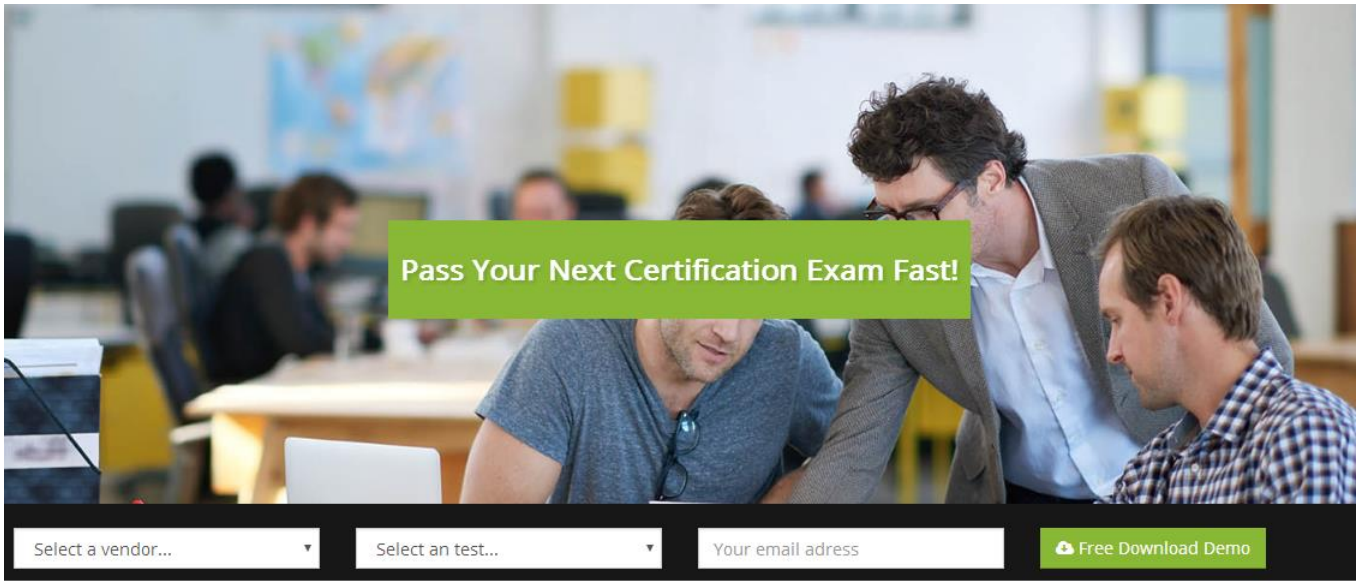
ITPassLeader



Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.itpassleader.com

High-praise Exam Dumps Questions grant you success by high pass rate - ITPassLeader

Exam : **PCCET**

Title : Palo Alto Networks Certified Cybersecurity Entry-level Technician

Vendor : Palo Alto Networks

Version : DEMO

NO.1 From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

A. Unit 52

B. PAN-DB

C. BrightCloud

D. MineMeld

Answer: B

Explanation:

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

NO.2 How does Prisma SaaS provide protection for Sanctioned SaaS applications?

A. Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility

B. Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure

C. Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility

D. Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

Answer: D

Explanation:

Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

NO.3 How can local systems eliminate vulnerabilities?

A. Patch systems and software effectively and continuously.

B. Create preventative memory-corruption techniques.

C. Perform an attack on local systems.

D. Test and deploy patches on a focused set of systems.

Answer: A

Explanation:

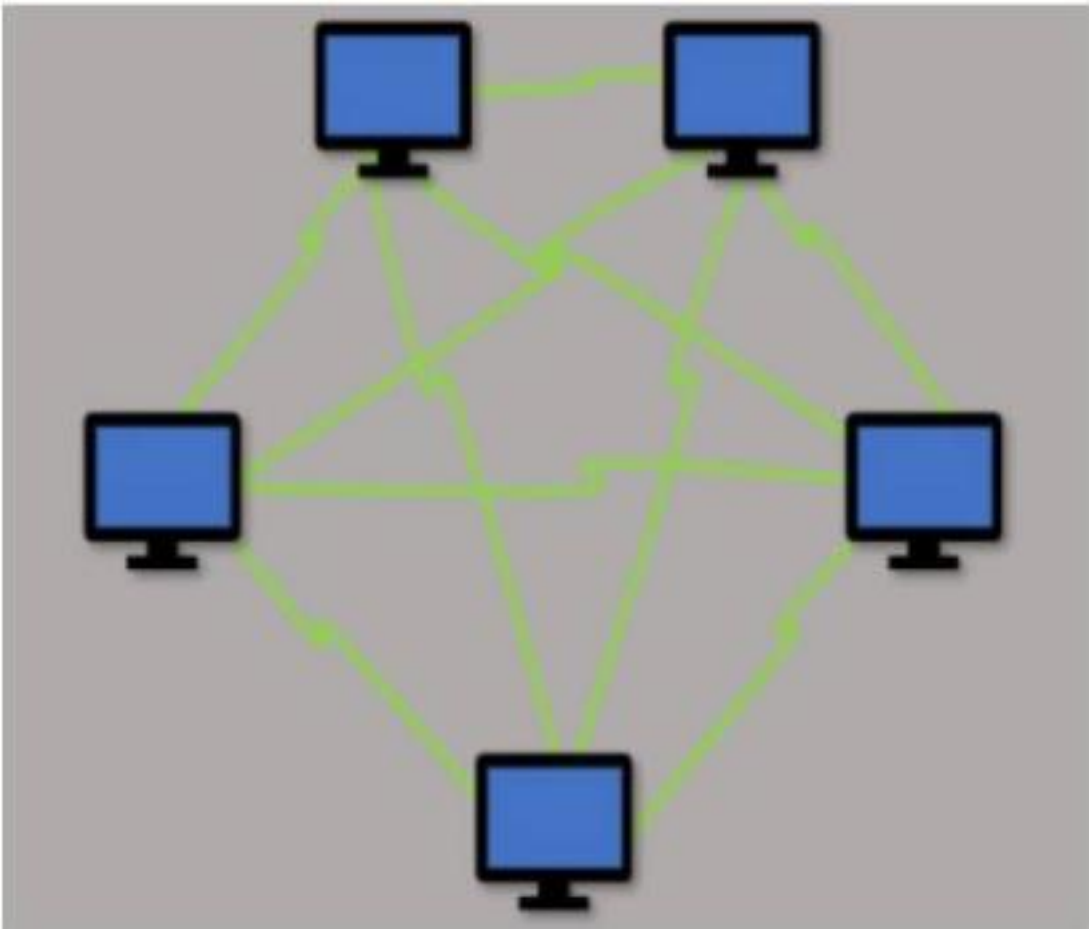
Local systems can eliminate vulnerabilities by patching systems and software effectively and continuously. Patching is the process of applying updates or fixes to software or hardware components that have known vulnerabilities or bugs. Patching can prevent attackers from exploiting these vulnerabilities and compromising the security or functionality of the systems. Patching should be done regularly and promptly, as new vulnerabilities are constantly discovered and exploited by cybercriminals. Patching should also be done effectively, meaning that the patches are tested and verified before deployment, and that they do not introduce new vulnerabilities or issues. Patching should also be done continuously, meaning that the systems are monitored for new vulnerabilities and patches are applied as soon as they are available. Continuous patching can reduce the window of opportunity for attackers to exploit unpatched vulnerabilities and cause damage or data breaches.

Reference:

* 1: What is Patch Management? | Palo Alto Networks

* 2: Patch Management Best Practices: How to Keep Your Systems Secure | Snyk
* 3: Vulnerability Remediation Process - 4 Steps to Remediation | Snyk

NO.4 Which type of LAN technology is being displayed in the diagram?



A. Star Topology
B. Spine Leaf Topology
C. Mesh Topology
D. Bus Topology
Answer: C
Explanation:
The diagram displays a mesh topology, where each device is connected to every other device in the network. This topology is characterized by the multiple connections each node has, ensuring there is no single point of failure and providing redundant paths for data transmission, enhancing the reliability and resilience of the network. Mesh topology is one of the types of LAN technology that uses ethernet or Wi-Fi to connect devices12. Reference:
What Is Local Area Network (LAN)? Definition, Types, Architecture, and Best Practices from Spiceworks Types of LAN | Introduction and Classification of LAN from EDUCBA

NO.5 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.

NO.6 What type of area network connects end-user devices?

A. Wide Area Network (WAN)

B. Campus Area Network (CAN)

C. Local Area Network (LAN)

D. Personal Area Network (PAN)

Answer: C

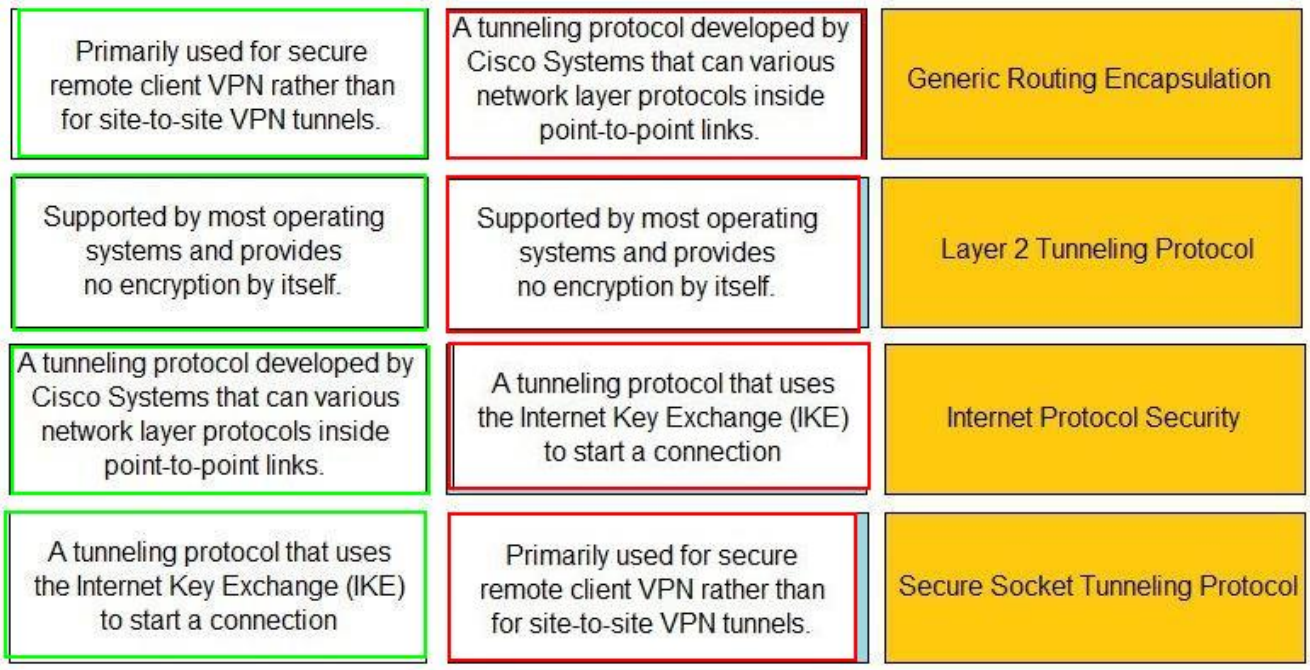
Explanation:

A local area network (LAN) is a network that connects end-user devices such as personal computers, printers, scanners, and phones within a small geographic area, such as an office, school, or home. LANs allow users to share resources, such as files, applications, and internet access, among the connected devices. LANs typically use Ethernet or Wi-Fi as the communication medium and operate at high speeds with low error rates. LANs are usually owned and managed by a single person or organization. Reference: LANs, WANs, and Other Area Networks Explained, What is a LAN? Local Area Network, Types of area networks - LAN, MAN and WAN

NO.7 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

Answer:



NO.8 An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?
Requirements for the three subnets: Subnet 1: 3 host addresses
Subnet 2: 25 host addresses
Subnet 3: 120 host addresses

A. 192.168.6.168/30

B. 192.168.6.0/25

C. 192.168.6.160/29

D. 192.168.6.128/27

Answer: B

Explanation:
To maximize the use of a network address, the administrator should use the subnet that can accommodate the required number of hosts with the least amount of wasted IP addresses. The subnet mask determines how many bits are used for the network portion and the host portion of the IP address. The more bits are used for the network portion, the more subnets can be created, but the fewer hosts can be assigned to each subnet. The formula to calculate the number of hosts per subnet is
2(32-n)-2
, where
n
is the number of bits in the network portion of the subnet mask. For example, a /30 subnet mask has 30 bits in the network portion, so the number of hosts per subnet is
2(32-30)-2=2
. A /25 subnet mask has 25 bits in the network portion, so the number of hosts per subnet is
2(32-25)-2=126
.
The subnet 192.168.6.0/25 can accommodate 126 hosts, which is enough for the network with 120

hosts. The subnet 192.168.6.168/30 can only accommodate 2 hosts, which is not enough. The subnet 192.168.6.160/29 can accommodate 6 hosts, which is also not enough. The subnet 192.168.6.128/27 can accommodate 30 hosts, which is enough, but it wastes more IP addresses than the /25 subnet. Therefore, the best option is B. 192.168.6.0/25. Reference:
Getting Started: Layer 3 Subinterfaces - Palo Alto Networks Knowledge Base DotW: Multiple IP Addresses on an Interface - Palo Alto Networks Knowledge Base Configure NAT - Palo Alto Networks | TechDocs

NO.9 Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?
A. UDP
B. MAC
C. SNMP
D. NFS
Answer: C
Explanation:
Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication.
Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system.
Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release.
Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.

NO.10 What are three benefits of the cloud native security platform? (Choose three.)
A. Increased throughput
B. Exclusivity
C. Agility
D. Digital transformation
E. Flexibility
Answer: C,D,E
Explanation:
A cloud native security platform (CNSP) is a set of security practices and technologies designed specifically for applications built and deployed in cloud environments. It involves a shift in mindset from traditional security approaches, which often rely on network-based protections, to a more application-focused approach that emphasizes identity and access management, container security and workload security, and continuous monitoring and response. A CNSP offers three main benefits for cloud native applications:
Agility: A CNSP enables faster and more frequent delivery of software updates, as security is built into the application and infrastructure from the ground up, rather than added on as an afterthought. This allows for seamless integration of security controls into the continuous integration/continuous delivery (CI/CD) pipeline, reducing the risk of security gaps or delays. A CNSP also leverages

automation and orchestration to simplify and streamline security operations, such as configuration, patching, scanning, and remediation.
Digital transformation: A CNSP supports the adoption of cloud native technologies, such as microservices, containers, serverless, and platform as a service (PaaS), which enable greater scalability, deployability, manageability, and performance of cloud applications. These technologies also allow for more innovation and experimentation, as developers can easily create, test, and deploy new features and functionalities. A CNSP helps to protect these cloud native architectures from threats and vulnerabilities, while also ensuring compliance with regulations and standards.
Flexibility: A CNSP provides consistent and comprehensive security across different cloud environments, such as public, private, and multi-cloud. It also allows for customization and adaptation of security policies and controls to suit the specific needs and preferences of each application and organization. A CNSP can also integrate with other security tools and platforms, such as firewalls, endpoint protection, threat intelligence, and security information and event management (SIEM), to provide a holistic and unified view of the security posture and risk level of cloud applications.
Reference:
What Is a Cloud Native Security Platform?
What Is Cloud-Native Security?
All You Need to Know About Cloud Native Security
Top Five Benefits of Cloud Native Application Security

NO.11 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"

NO.12 Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

A. Network

B. Management

C. Cloud

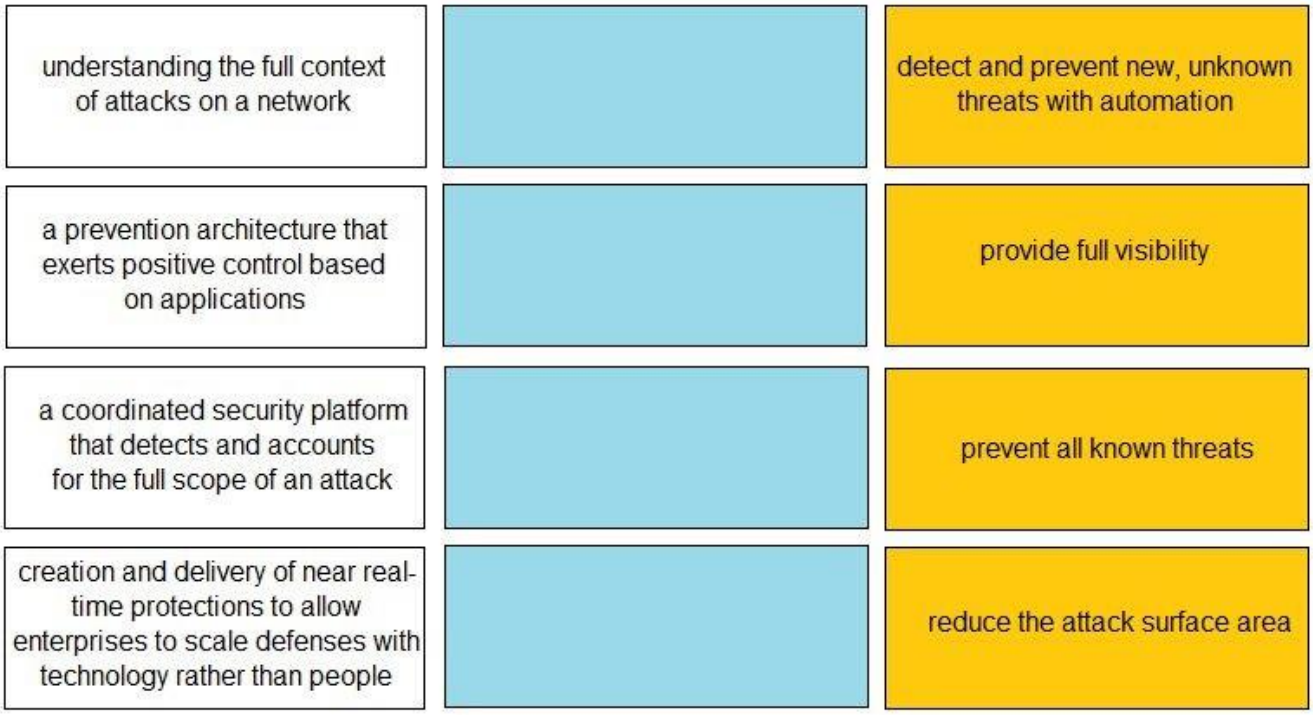
D. Security

Answer: D

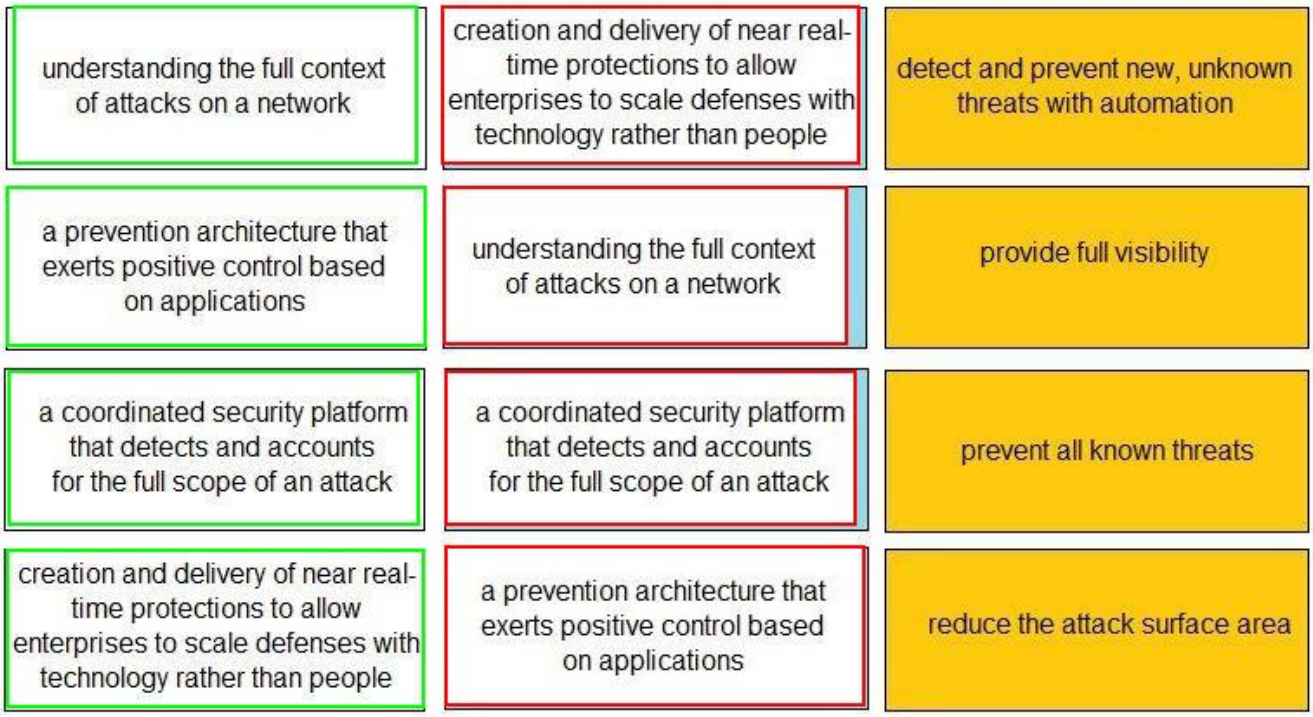
Explanation:
A SASE solution converges networking and security services into one unified, cloud-delivered solution

(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)

NO.13 Match each description to a Security Operating Platform key capability.



Answer:



NO.14 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

Explanation:

Sanctioned SaaS applications are those that are approved and supported by the organization's IT department. They provide business benefits such as increased productivity, collaboration, and efficiency. They are fast to deploy because they do not require installation or maintenance on the user's device. They require minimal cost because they are usually paid on a subscription or usage basis, and they do not incur hardware or software expenses. They are infinitely scalable because they can adjust to the changing needs and demands of the organization without affecting performance or availability12. Reference: 8 Types of SaaS Solutions You Must Know About in 2024, What is SaaS (Software as a Service)? | SaaS Types | CDW, Palo Alto Networks Certified Cybersecurity Entry-level Technician

NO.15 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

NO.16 Which action must Secunty Operations take when dealing with a known attack?

A. Document, monitor, and track the incident.

B. Limit the scope of who knows about the incident.

C. Increase the granularity of the application firewall.

D. Disclose details of lhe attack in accordance with regulatory standards.

Answer: A

Explanation:
Security Operations (SecOps) is the process of coordinating and aligning security teams and IT teams to improve the security posture of an organization. SecOps involves implementing and maintaining security controls, technologies, policies, and procedures to protect the organization from cyber threats and incidents. When dealing with a known attack, SecOps must take the following action: document, monitor, and track the incident. This action is important because it helps SecOps to:
* Record the details of the attack, such as the source, target, impact, timeline, and response actions.
* Monitor the status and progress of the incident response and recovery efforts, as well as the ongoing threat activity and indicators of compromise.
* Track the performance and effectiveness of the security controls and technologies, as well as the lessons learned and improvement opportunities. Reference:
* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
* 6 Incident Response Steps to Take After a Security Event - Exabeam
* Dealing with Cyber Attacks-Steps You Need to Know | NIST