Practice Exam Questions

Palo Alto Networks Certified Cyber Security Entry-level Technician

EXAMKILLER

Help Pass Your Exam At First Try

Paloalto Networks

Exam PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Version: 5.0

[Total Questions: 145]

Question No : 1

What are three benefits of SD-WAN infrastructure? (Choose three.)

A. Improving performance of SaaS applications by requiring all traffic to be back-hauled through the corporate headquarters network
B. Promoting simplicity through the utilization of a centralized management structure
C. Utilizing zero-touch provisioning for automated deployments
D. Leveraging remote site routing technical support by relying on MPLS
E. Improving performance by allowing efficient access to cloud-based resources without requiring back-haul traffic to a centralized location

Answer: B,C,E

Explanation:

Simplicity: Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites. Improved performance: By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.

Question No : 2

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

Question No : 3

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)

Question No : 4

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

Question No : 5

Which technique uses file sharing or an instant messenger client such as Meebo running over Hypertext Transfer Protocol (HTTP)?

A. Use of non-standard ports
B. Hiding within SSL encryption
C. Port hopping
D. Tunneling within commonly used services

Answer: D

Question No : 6

What is the purpose of SIEM?

A. Securing cloud-based applications
B. Automating the security team's incident response
C. Real-time monitoring and analysis of security events
D. Filtering webpages employees are allowed to access

Answer: C

Question No : 7

You have been invited to a public cloud design and architecture session to help deliver secure east west flows and secure Kubernetes workloads.

What deployment options do you have available? (Choose two.)

A. PA-Series
B. VM-Series
C. Panorama
D. CN-Series

Answer: A,B

Question No : 8

What does SIEM stand for?

A. Security Infosec and Event Management
B. Security Information and Event Management
C. Standard Installation and Event Media
D. Secure Infrastructure and Event Monitoring

Answer: B

Explanation: Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades

Question No : 9

On which security principle does virtualization have positive effects?

A. integrity
B. confidentiality
C. availability
D. non-repudiation

Answer: C

Question No : 10

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

A. North-South traffic
B. Intrazone traffic
C. East-West traffic
D. Interzone traffic

Answer: A

Question No : 11

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: 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

Question No : 12

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.

Question No : 13

Web 2.0 applications provide which type of service?

A. SaaS
B. FWaaS
C. IaaS
D. PaaS

Answer: D

Question No : 14

Which type of malware takes advantage of a vulnerability on an endpoint or server?

A. technique
B. patch
C. vulnerability
D. exploit

Answer: A

Question No : 15

Which aspect of a SaaS application requires compliance with local organizational security policies?

A. Types of physical storage media used
B. Data-at-rest encryption standards
C. Acceptable use of the SaaS application
D. Vulnerability scanning and management

Answer: C

Question No : 16

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.

Question No : 17

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"

Question No : 18

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

Question No : 19

Which network firewall primarily filters traffic based on source and destination IP address?

A. Proxy
B. Stateful
C. Stateless
D. Application

Answer: B

Question No : 20

What should a security operations engineer do if they are presented with an encoded string

during an incident investigation?

A. Save it to a new file and run it in a sandbox.
B. Run it against VirusTotal.
C. Append it to the investigation notes but do not alter it.
D. Decode the string and continue the investigation.

Answer: D

Question No : 21

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

Question No : 22 DRAG DROP

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

Question No : 23

Which of the following is a Routed Protocol?

A. Routing Information Protocol (RIP)
B. Transmission Control Protocol (TCP)
C. Internet Protocol (IP)
D. Domain Name Service (DNS)

Answer: A

Question No : 24

Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

A. Statistical-based
B. Knowledge-based
C. Behavior-based
D. Anomaly-based

Answer: B

Explanation: A knowledge-based system uses a database of known vulnerabilities and attack profiles
to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.
A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

Question No : 25

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.

Question No : 26

Which type of IDS/IPS uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt?

A. Knowledge-based
B. Signature-based
C. Behavior-based
D. Database-based

Answer: C

Explanation:

IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems:

A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.

A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems

Question No : 27

Which of the following is an AWS serverless service?

A. Beta
B. Kappa
C. Delta
D. Lambda

Answer: D

Explanation:

Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

Question No : 28

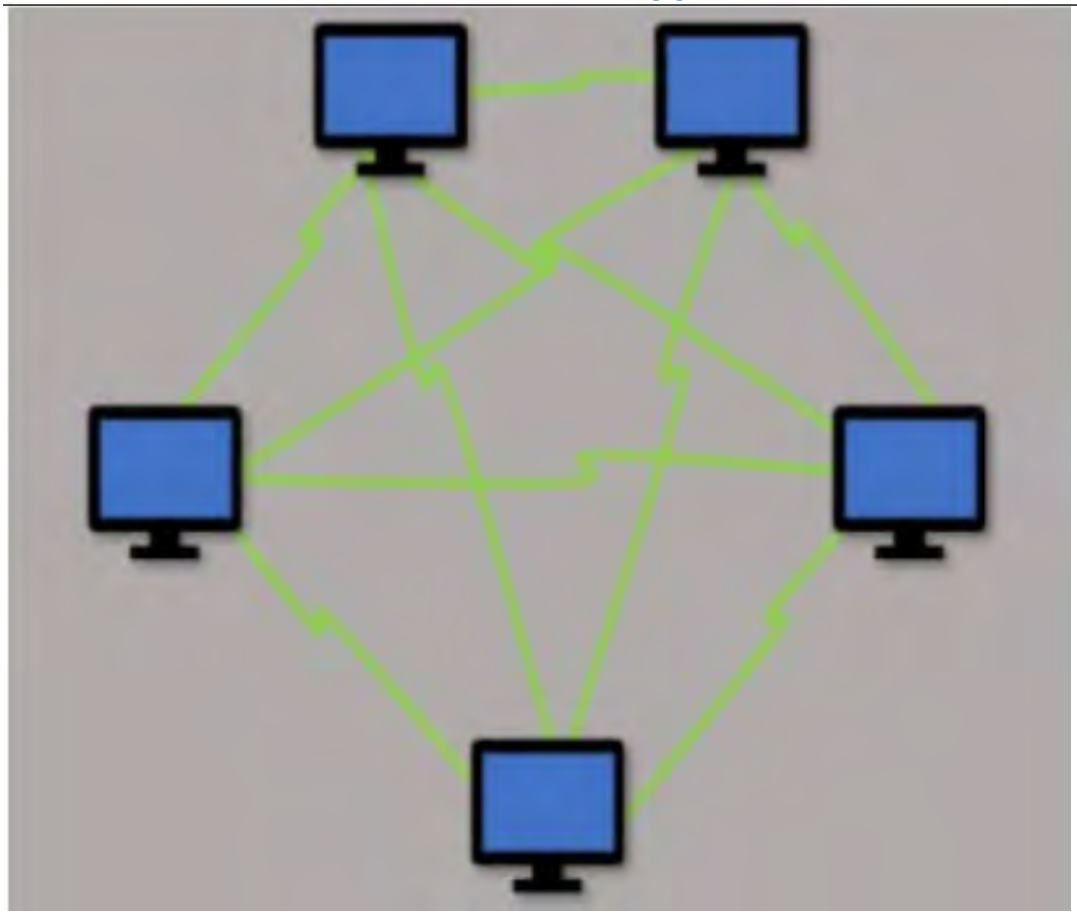
Which native Windows application can be used to inspect actions taken at a specific time?

A. Event Viewer
B. Timeline inspector
C. Task Manager
D. Task Scheduler

Answer: A

Question No : 29

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: A

Question No : 30

Which activities do local organization security policies cover for a SaaS application?

A. how the data is backed up in one or more locations
B. how the application can be used
C. how the application processes the data
D. how the application can transit the Internet

Answer: B