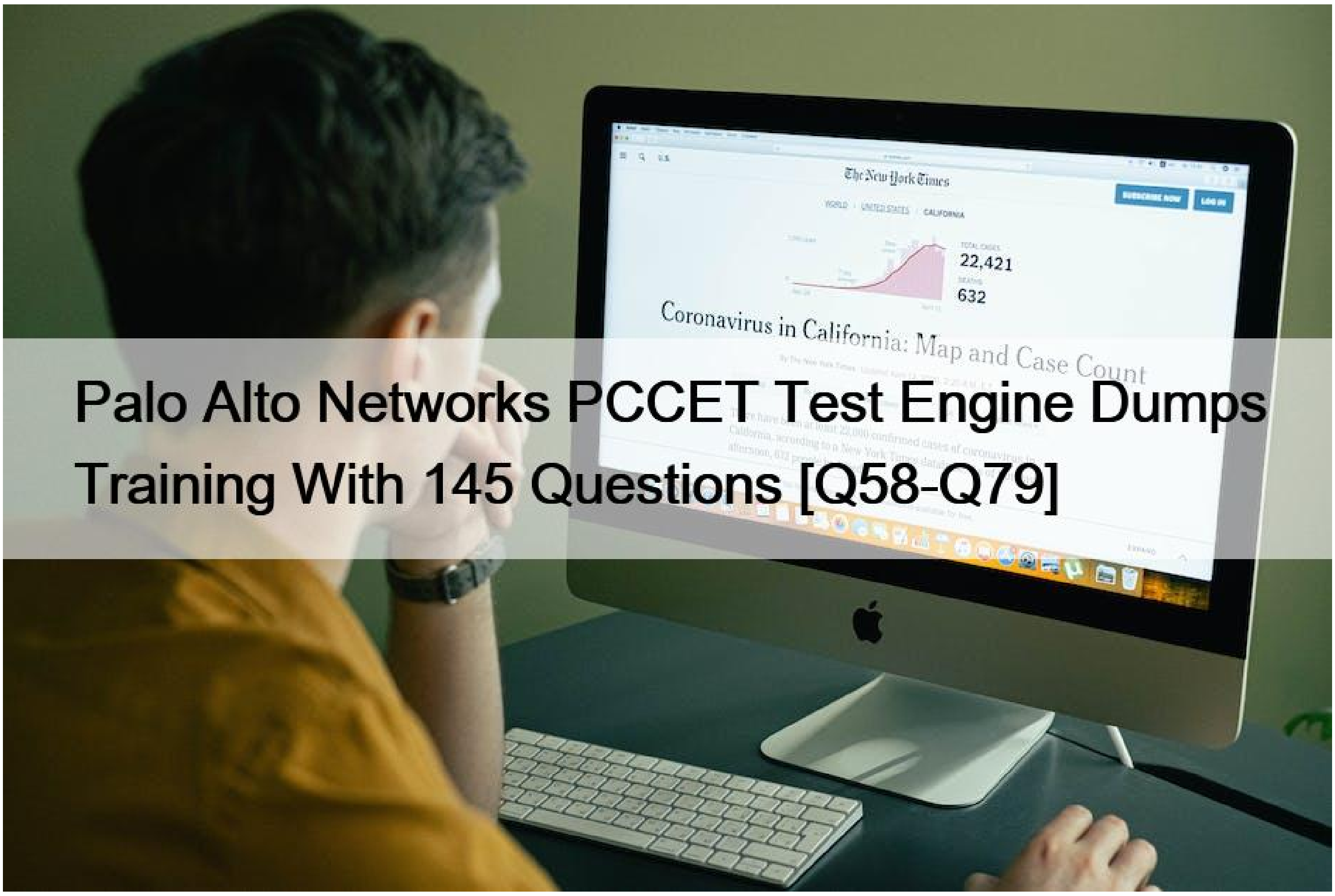
Palo Alto Networks PCCET Test Engine Dumps Training With 145 Questions [Q58-Q79



Palo Alto Networks PCCET Test Engine Dumps Training With 145 Questions
PCCET Questions Pass on Your First Attempt Dumps for Certified Cybersecurity Associate Certified

The PCCET certification exam is an online proctored exam that consists of 75 multiple-choice questions. PCCET exam has a duration of 90 minutes, and the passing score is 70%. PCCET exam is available in English and Japanese languages. PCCET exam fee is $100, and it can be taken from anywhere in the world. Palo Alto Networks Certified Cybersecurity Entry-level Technician certification is valid for two years, and individuals need to retake the exam to renew their certification.

NEW QUESTION 58

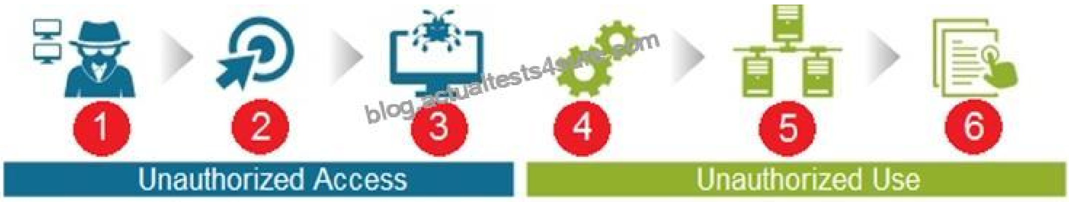
During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?
* Frame
* Segment
* Packet

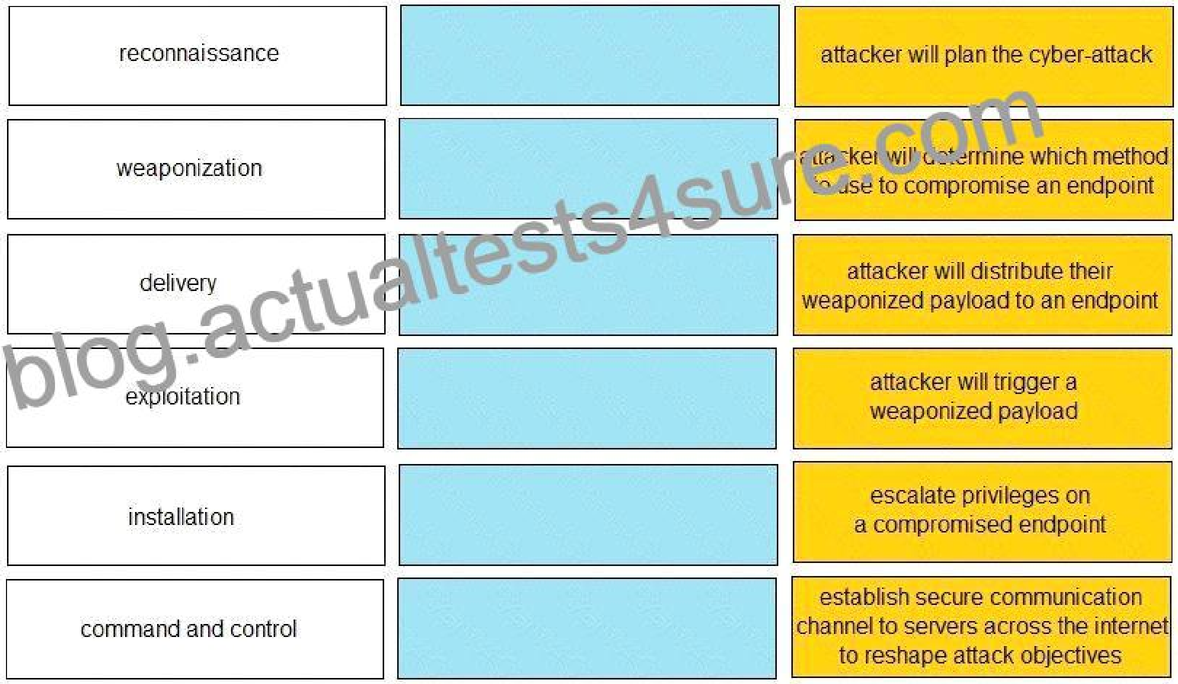
* Data

The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.

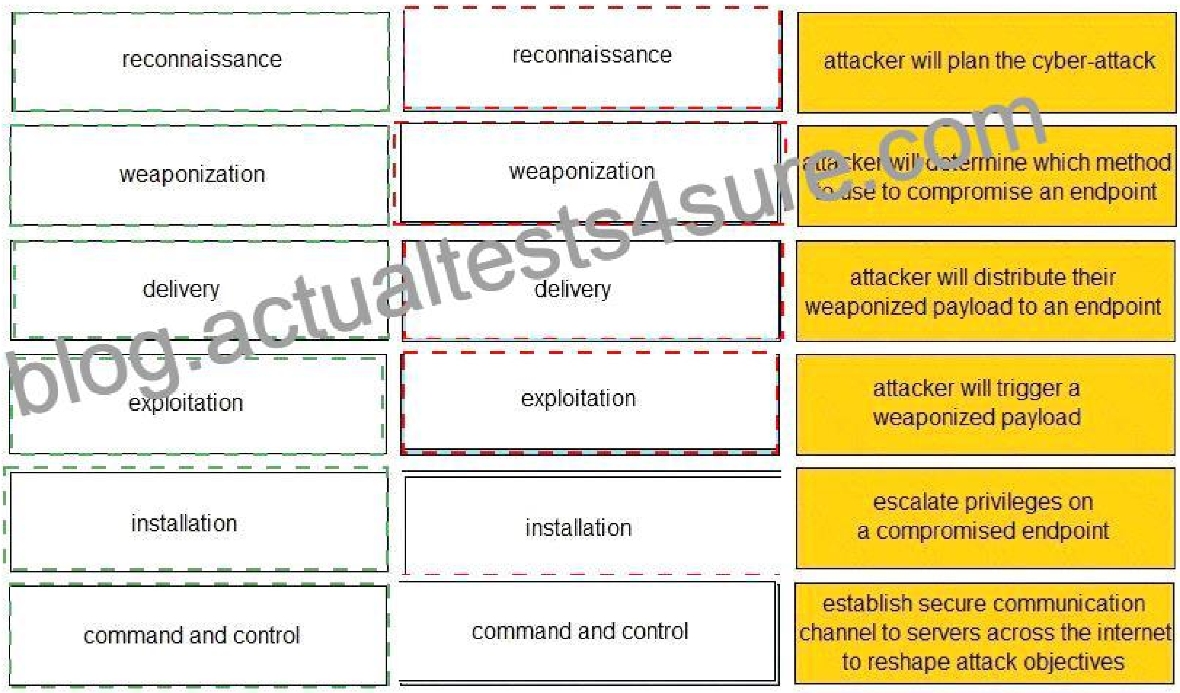
NEW QUESTION 59

Given the graphic, match each stage of the cyber-attack lifecycle to its description.

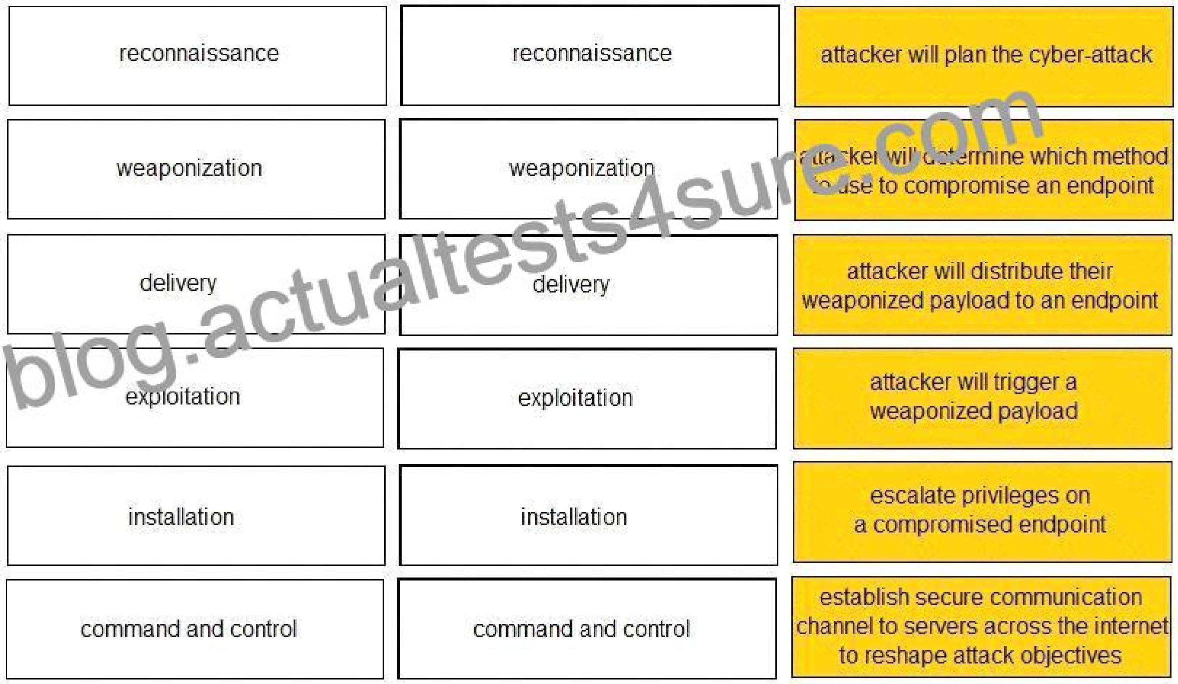




reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives



reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives



reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

NEW QUESTION 60

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?

* Group policy
* Stateless
* Stateful

* Static packet-filter
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&#8217;t inspected after the connection is established.

NEW QUESTION 61

In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?
* the network is large
* the network is small
* the network has low bandwidth requirements
* the network needs backup routes
A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can&#8217;t be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can&#8217;t be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that&#8217;s used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn&#8217;t broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

NEW QUESTION 62

Which option describes the &#8220;selective network security virtualization&#8221; phase of incrementally transforming data centers?
* during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
* during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
* during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
* during the selective network security virtualization phase, all intra-host traffic is load balanced
Selective network security virtualization: Intra-host communications and live migrations are architected at this phase. All intra-host communication paths are strictly controlled to ensure that traffic between VMs at different trust levels is intermediated either by an on-box, virtual security appliance or by an off-box, physical security appliance.

NEW QUESTION 63

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?
* exploitation
* actions on the objective
* command and control
* installation
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.

NEW QUESTION 64

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?
* Cortex XDR
* AutoFocus
* MineMild
* Cortex XSOAR
In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.

NEW QUESTION 65

Which tool supercharges security operations center (SOC) efficiency with the world&#8217;s most comprehensive operating platform for enterprise security?
* Prisma SAAS
* WildFire
* Cortex XDR
* Cortex XSOAR

NEW QUESTION 66

Which key component is used to configure a static route?
* router ID
* enable setting
* routing protocol
* next hop IP address

NEW QUESTION 67

Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?
* Statistical-based
* Knowledge-based
* Behavior-based
* Anomaly-based
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.

NEW QUESTION 68

Which method is used to exploit vulnerabilities, services, and applications?
* encryption
* port scanning
* DNS tunneling
* port evasion
Explanation

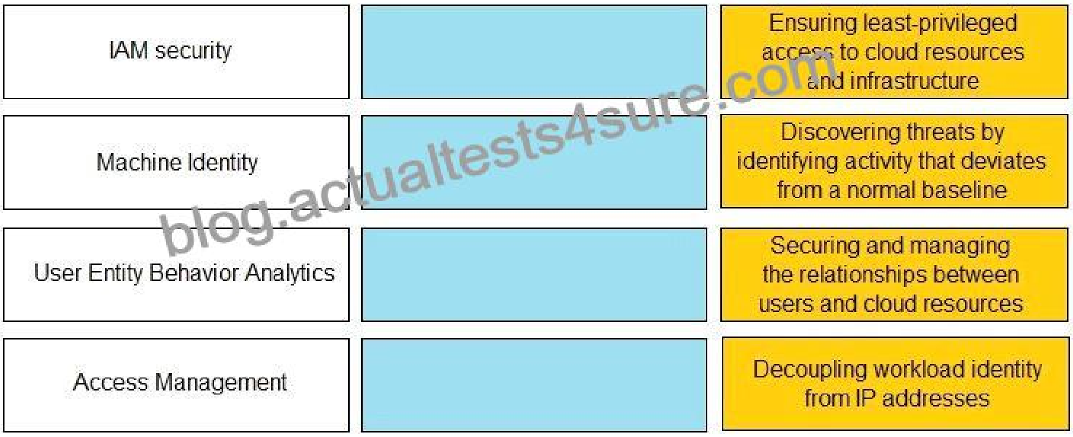
Attack communication traffic is usually hidden with various techniques and tools, including:

Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic.

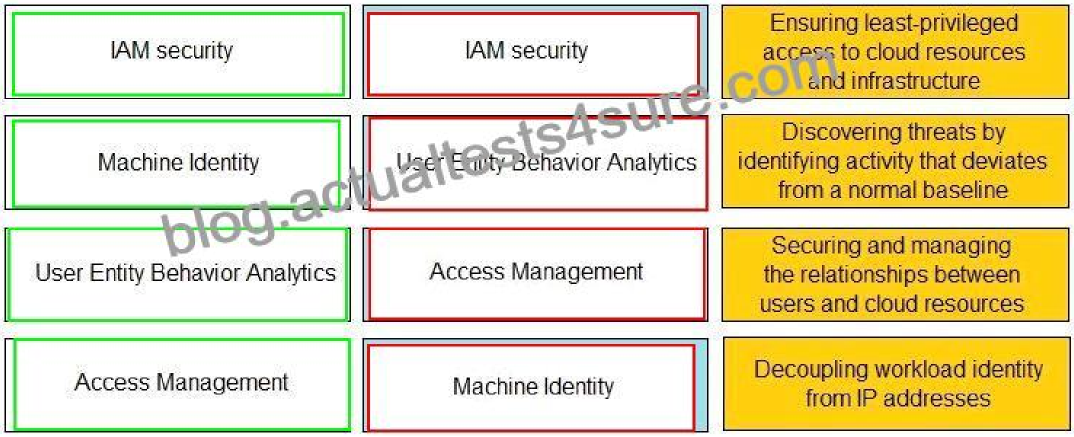
Port evasion using network anonymizers or port hopping to traverse over any available open ports Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult DNS tunneling is used for C2 communications and data infiltration

NEW QUESTION 69

Match the Identity and Access Management (IAM) security control with the appropriate definition.



IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses



IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

NEW QUESTION 70

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?
* Knowledge-based
* Signature-based
* Behavior-based
* Database-based
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

NEW QUESTION 71

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?
* SaaS
* DaaS
* PaaS
* IaaS

NEW QUESTION 72

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

* Network
* Management
* Cloud
* Security

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)

NEW QUESTION 73

Which option is an example of a North-South traffic flow?

* Lateral movement within a cloud or data center
* An internal three-tier application
* Client-server interactions that cross the edge perimeter
* Traffic between an internal server and internal user

North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.

NEW QUESTION 74

In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

* Computer
* Switch
* Infrastructure

* Cloud
Cortex XDR breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks

NEW QUESTION 75

Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?
* MineMeld
* AutoFocus
* WildFire
* Cortex XDR
&#8220;Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team&#8217;s existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources.&#8221;

NEW QUESTION 76

In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?
* Computer
* Switch
* Infrastructure
* Cloud
Explanation

Cortex XDR breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks

NEW QUESTION 77

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?
* control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
* control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
* control and protect inter-host traffic by using IPv4 addressing
* control and protect inter-host traffic using physical network security appliances
Explanation

page 211 &#8220;Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: &#8230; &#8230; &#8230; This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus.&#8221;

NEW QUESTION 78

You received an email, allegedly from a bank, that asks you to click a malicious link to take action on your account.

Which type of attack is this?

* Whaling
* Spamming
* Spear phishing
* Phishing

NEW QUESTION 79

Which endpoint tool or agent can enact behavior-based protection?
* AutoFocus
* Cortex XDR
* DNS Security
* MineMeld
Explanation

PCCET Practice Test Pdf Exam Material: https://www.actualtests4sure.com/PCCET-test-questions.html]