Exam	:	**PSE-SASE**
Title	:	Palo Alto Networks Accredited Systems Engineer (PSE) - SASE Professional
Vendor	:	Palo Alto Networks
Version	:	V12.35

NO.1 The Cortex Data Lake sizing calculator for Prisma Access requires which three values as inputs? (Choose three.)

A. throughput of remote networks purchased

B. cloud-managed or Panorama-managed deployment

C. retention period for the logs to be stored

D. number of log-forwarding destinations

E. number of mobile users purchased

Answer: A C E

NO.2 Which product enables organizations to open unknown files in a sandbox environment and scan them for malware or other threats?

A. network sandbox

B. SD-WAN

C. cloud access security broker (CASB)

D. remote browser isolation

Answer: A

NO.3 How can a network engineer export all flow logs and security actions to a security information and event management (SIEM) system?

A. Enable syslog on the Instant-On Network (ION) device.

B. Use a zone-based firewall to export directly through application program interface (API) to the SIEM.

C. Enable Simple Network Management Protocol (SNMP) on the Instant-On Network (ION) device.

D. Use the centralized flow data-export tool built into the controller.

Answer: A

NO.4 How does SaaS Security Inline provide a consistent management experience?

A. user credentials required before accessing the resource

B. uses advanced predictive analysis and machine learning (ML)

C. automatically forwards samples for WildFire analysis

D. integrates with existing security

Answer: D

NO.5 Which statement describes the data loss prevention (DLP) add-on?

A. It prevents phishing attacks by controlling the sites to which users can submit valid corporate credentials.

B. It employs automated policy enforcement to allow trusted behavior with a new Device-ID policy construct.

C. It is a centrally delivered cloud service with unified detection policies that can be embedded in existing control points.

D. It enables data sharing with third-party tools such as security information and event management (SIEM) systems.

Answer: C

NO.6 How does the Palo Alto Networks secure access service edge (SASE) solution enable Zero Trust in a customer environment?

A. It stops attacks that use DNS for command and control or data theft.

B. It feeds threat intelligence into an automation engine for rapid and consistent protections.

C. It classifies sites based on content, features, and safety.

D. It continuously validates every stage of a digital interaction.

Answer: D

NO.7 Which product leverages GlobalProtect agents for endpoint visibility and native Prisma SD-WAN integration for remote sites and branches?

A. Cloud-Delivered Security Services (CDSS)

B. WildFire

C. CloudBlades:

D. Autonomous Digital Experience Management (ADEM)

Answer: A

NO.8 How does SaaS Security Inline help prevent the data security risks of unsanctioned security-as-a-service (SaaS) application usage on a network?

A. It provides mobility solutions and/or large-scale virtual private network (VPN) capabilities.

B. It offers risk scoring, analytics, reporting, and Security policy rule authoring.

C. It provides built-in external dynamic lists (EDLs) that secure the network against malicious hosts.

D. It prevents credential theft by controlling sites to which users can submit their corporate credentials.

Answer: C

NO.9 What are three ways the secure access service edge (SASE) model can help an organization? (Choose three.)

A. cost savings

B. data protection

C. increased licensing requirements

D. increased performance

E. decreased reliance on best practices

Answer: A B D

NO.10 What is an advantage of the unified approach of the Palo Alto Networks secure access service edge (SASE) platform over the use of multiple point products?

A. It allows for automation of ticketing tasks and management of tickets without pivoting between various consoles.

B. It scans all traffic, ports, and protocols and automatically discovers new apps.

C. It turns threat intelligence and external attack surface data into an intelligent data foundation to dramatically accelerate threat response.

D. It reduces network and security complexity while increasing organizational agility.

Answer: D

NO.11 A customer currently has 150 Mbps of capacity at a site. Records show that, on average, a total of 30 Mbps of bandwidth is used for the two links.
What is the appropriate Prisma SD-WAN license for this site?

A. 50 Mbps
B. 175 Mbps
C. 250 Mbps
D. 25 Mbps
Answer: A

NO.12 What is an advantage of next-generation SD-WAN over legacy SD-WAN solutions?

A. It enables definition of the privileges and responsibilities of administrative users in a network.
B. It allows configuration to forward logs to external logging destinations, such as syslog servers.
C. It steers traffic and defines networking and security policies from an application-centric perspective, rather than a packet-based approach.
D. It provides the ability to push common configurations, configuration updates, and software upgrades to all or a subset of the managed appliances.
Answer: C

NO.13 Which statement applies to Prisma Access licensing?

A. Internet of Things (IOT) Security is included with each license.
B. It provides cloud-based, centralized log storage and aggregation.
C. It is a perpetual license required to enable support for multiple virtual systems on PA-3200 Series firewalls.
D. For remote network and Clean Pipe deployments, a unit is defined as 1 Mbps of bandwidth.
Answer: D

NO.14 Which elements of Autonomous Digital Experience Management (ADEM) help provide end-to-end visibility of everything in an organization's environment?

A. integrated threat intelligence management, automated distribution to enforcement points at scale, full ticket mirroring
B. scanning of all traffic, ports, and protocols
C. data collected from endpoint devices, synthetic monitoring tests, and real-time traffic
D. alerts, artifacts, and MITRE tactics
Answer: A

NO.15 Which product enables websites to be rendered in a sandbox environment in order to detect and remove malware and threats before they reach the endpoint?

A. remote browser isolation
B. secure web gateway (SWG)
C. network sandbox
D. DNS Security

Answer: B

NO.16 Which two services are part of the Palo Alto Networks cloud-delivered security services (CDSS) package?
(Choose two.)
A. virtual desktop infrastructure (VDI)
B. Internet of Things (IoT) Security
C. Advanced URL Filtering (AURLF)
D. security information and event management (SIEM)
Answer: B C

NO.17 What is a disadvantage of proxy secure access service edge (SASE) when compared to an inline SASE solution?
A. Proxies force policy actions to be treated as business decisions instead of compromises due to technical limitations.
B. Teams added additional tools to web proxies that promised to solve point problems, resulting in a fragmented and ineffective security architecture.
C. Proxy solutions require an unprecedented level of interconnectivity.
D. Exclusive use of web proxies leads to significant blind spots in traffic and an inability to identify applications and threats on non-standard ports or across multiple protocols.
Answer: D

NO.18 What is an advantage of the Palo Alto Networks cloud-based security infrastructure?
A. It provides comprehensive, scalable cloud security with flexible licensing options.
B. It backhauls traffic to the corporate network.
C. It allows for the elimination of data centers within five years of implementation.
D. It increases the footprint of the security solution.
Answer: A

NO.19 In an SD-WAN deployment, what allows customers to modify resources in an automated fashion instead of logging on to a central controller or using command-line interface (CLI) to manage all their configurations?
A. dynamic user group (DUG)
B. DNS server
C. application programming interface (API)
D. WildFire
Answer: A

NO.20 Cloud-delivered App-ID provides specific identification of which two applications? (Choose two.)
A. unknown-tcp
B. private
C. web-browsing

D. custom
Answer: A C

NO.21 Which element of a secure access service edge (SASE)-enabled network uses many points of presence to reduce latency with support of in-country or in-region resources and regulatory requirements?
A. cloud-native, cloud-based delivery
B. converged WAN edge and network security
C. broad network-edge support
D. identity and network location
Answer: A

NO.22 In the aggregate model, how are bandwidth allocations and interface tags applied beginning in Prisma Access
1.8?
A. License bandwidth is allocated to a CloudGenix controller; interface tags are set with a compute region.
B. License bandwidth is allocated to a compute region; interface tags are set with a CloudGenix controller.
C. License bandwidth is allocated to a compute region; interface tags are set with a Prisma Access location.
D. License bandwidth is allocated to a Prisma Access location; interface tags are set with a compute region.
Answer: C

NO.23 What are two benefits provided to an organization using a secure web gateway (SWG)? (Choose two.)
A. VPNs remain connected, reducing user risk exposure.
B. Security policies for making internet access safer are enforced.
C. Access to inappropriate websites or content is blocked based on acceptable use policies.
D. An encrypted challenge-response mechanism obtains user credentials from the browser.
Answer: B C

NO.24 Which product continuously monitors each segment from the endpoint to the application and identifies baseline metrics for each application?
A. App-ID Cloud Engine (ACE)
B. Autonomous Digital Experience Management (ADEM)
C. CloudBlades
D. WildFire
Answer: B

NO.25 Which element of Prisma Access enables both mobile users and users at branch networks to access resources in headquarters or a data center?
A. User-ID

B. private clouds
C. App-ID
D. service connections
Answer: D

NO.26 In which step of the Five-Step Methodology of Zero Trust are application access and user access defined?
A. Step 4: Create the Zero Trust Policy
B. Step 3: Architect a Zero Trust Network
C. Step 1: Define the Protect Surface
D. Step 5: Monitor and Maintain the Network
Answer: A

NO.27 Which two point products are consolidated into the Prisma secure access service edge (SASE) platform?
(Choose two.)
A. Autonomous Digital Experience Management (ADEM)
B. firewall as a service (FWaaS)
C. Threat Intelligence Platform (TIP)
D. security information and event management (SIEM)
Answer: A B

NO.28 What is a benefit of a cloud-based secure access service edge (SASE) infrastructure over a Zero Trust Network Access (ZTNA) product based on a software-defined perimeter (SDP) model?
A. Users, devices, and apps are identified no matter where they connect from.
B. Connection to physical SD-WAN hubs in ther locations provides increased interconnectivity between branch offices.
C. Complexity of connecting to a gateway is increased, providing additional protection.
D. Virtual private network (VPN) services are used for remote access to the internal data center, but not the cloud.
Answer: A

NO.29 Which product draws on data collected through PAN-OS device telemetry to provide an overview of the health of an organization's next-generation firewall (NGFW) deployment and identify areas for improvement?
A. Cloud Identity Engine (CIE)
B. DNS Security
C. security information and event management (SIEM)
D. Device Insights
Answer: D

NO.30 What is a benefit of deploying secure access service edge (SASE) with a secure web gateway (SWG) over a SASE solution without a SWG?

A. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down.
B. It prepares the keys and certificates required for decryption, creating decryption profiles and policies, and configuring decryption port mirroring.
C. Protection is offered in the cloud through a unified platform for complete visibility and precise control over web access while enforcing security policies that protect users from hostile websites.
D. It creates tunnels that allow users and systems to connect securely over a public network as if they were connecting over a local area network (LAN).
Answer: C

NO.31 What can prevent users from unknowingly downloading potentially malicious file types from the internet?
A. Apply a File Blocking profile to Security policy rules that allow general web access.
B. Apply a Zone Protection profile to the untrust zone.
C. Assign an Antivirus profile to Security policy rules that deny general web access.
D. Assign a Vulnerability profile to Security policy rules that deny general web access.
Answer: A

NO.32 Which type of access allows unmanaged endpoints to access secured on-premises applications?
A. manual external gateway
B. secure web gateway (SWG)
C. GlobalProtect VPN for remote access
D. Prisma Access Clientless VPN
Answer: D

NO.33 What is a differentiator between the Palo Alto Networks secure access service edge (SASE) solution and competitor solutions?
A. path analysis
B. playbooks
C. ticketing systems
D. inspections
Answer: A

NO.34 Which two services are part of the Palo Alto Networks cloud-delivered security services (CDSS) package?
(Choose two.)
A. Internet of Things (IoT) Security
B. virtual desktop infrastructure (VDI)
C. Advanced URL Filtering (AURLF)
D. security information and event management (SIEM)
Answer: A,C

NO.35 Which secure access service edge (SASE) networking component inspects web-based protocols and traffic to securely connect users to applications?

A. proxy

B. SD-WAN

C. secure web gateway (SWG)

D. cloud access security broker (CASB)

Answer: C

NO.36 Which component of the secure access service edge (SASE) solution provides complete session protection, regardless of whether a user is on or off the corporate network?

A. Zero Trust

B. threat prevention

C. single-pass architecture (SPA)

D. DNS Security

Answer: A

NO.37 A customer currently uses a third-party proxy solution for client endpoints and would like to migrate to Prisma Access to secure mobile user internet-bound traffic.
Which recommendation should the Systems Engineer make to this customer?

A. With the explicit proxy license add-on, set up GlobalProtect.

B. With the mobile user license, set up explicit proxy.

C. With the explicit proxy license, set up a service connection.

D. With the mobile user license, set up a corporate access node.

Answer: B

NO.38 In which step of the Five-Step Methodology for implementing the Zero Trust model are the services most valuable to the company defined?

A. Step 2: Map the transaction flows

B. Step 4: Create the Zero Trust policy

C. Step 5: Monitor and maintain the network

D. Step 1: Define the protect surface

Answer: D

NO.39 What is feature of Autonomous Digital Experience Management (ADEM)?

A. It applies configuration changes and provides credential management, role-based controls, and a playbook repository.

B. It provides customized forms to collect and validate necessary parameters from the requester.

C. It natively ingests, normalizes, and integrates granular data across the security infrastructure at nearly half the cost of legacy security products attempting to solve the problem.

D. It provides IT teams with single-pane visibility that leverages endpoint, simulated, and real-time user traffic data to provide the most complete picture of user traffic flows possible.

Answer: D

NO.40 Which App Response Time metric is the measure of network latency?
A. Round Trip Time (RTT)
B. Server Response Time (SRT)
C. Network Transfer Time (NTTn)
D. UDP Response Time (UDP-TRT)
Answer: A

NO.41 Which two services are provided by Prisma Access Insights? (Choose two.)
A. summary overview screen of the health and performance of an organization's entire Prisma Access environment
B. configuration of the on-premises firewall located behind the service-connection termination
C. detection of hard-to-find security issues via AI-based innovations to normalize, analyze, and stitch together an enterprise's data
D. multiple dashboards for focused views of different deployments, the corresponding alerts, and the health status of the infrastructure
Answer: A D

NO.42 How does Autonomous Digital Experience Management (ADEM) improve user experience?
A. The root cause of any alert can be viewed with a single click, allowing users to swiftly stop attacks across the environment.
B. The virtual appliance receives and stores firewall logs without using a local Log Collector, simplifying required steps users must take.
C. Working from home or branch offices, all users get the benefit of a digital experience management solution without the complexity of installing additional software and hardware.
D. It applies in-depth hunting and forensics knowledge to identify and contain threats before they become a breach.
Answer: C

NO.43 Which product allows advanced Layer 7 inspection, access control, threat detection and prevention?
A. Infrastructure as a Service (IaaS)
B. remote browser isolation
C. network sandbox
D. Firewall as a Service (FWaaS)
Answer: D

NO.44 How does a secure web gateway (SWG) protect users from web-based threats while still enforcing corporate acceptable use policies?
A. Users are mapped via server logs for login events and syslog messages from authenticating services.
B. It uses a cloud-based machine learning (ML)-powered web security engine to perform ML-based inspection of web traffic in real-time.
C. It prompts the browser to present a valid client certificate to authenticate the user.

D. Users access the SWG, which then connects the user to the website while still performing security measures.
Answer: D

NO.45 Which element of a secure access service edge (SASE)-enabled network provides true integration of services, not service chains, with combined services and visibility for all locations, mobile users, and the cloud?
A. identity and network location
B. broad network-edge support
C. converged WAN edge and network security
D. cloud-native, cloud-based delivery
Answer: D

NO.46 Which two key benefits have been identified for a customer investing in the Palo Alto Networks Prisma secure access service edge (SASE) solution? (Choose two.)
A. decreased likelihood of a data breach
B. reduced input required from management during third-party investigations
C. decreased need for interaction between branches
D. reduced number of security incidents requiring manual investigation
Answer: B D

NO.47 In which step of the Five-Step Methodology for implementing the Zero Trust model does inspection and logging of all traffic take place?
A. Step 4: Create the Zero Trust policy
B. Step 3: Architect a Zero Trust network
C. Step 1: Define the protect surface
D. Step 5: Monitor and maintain the network
Answer: D

NO.48 In which step of the Five-Step Methodology for implementing the Zero Trust model is the Kipling Method relevant?
A. Step 3: Architect a Zero Trust network
B. Step 5: Monitor and maintain the network
C. Step 4: Create the Zero Trust policy
D. Step 2: Map the transaction flows
Answer: C

NO.49 Which CLI command allows visibility into SD-WAN events such as path selection and path quality measurements?
A. >show sdwan connection all |
B. >show sdwan session distribution policy-name
C. >show sdwan path-monitor stats vif
D. >show sdwan event

Answer: D

NO.50 Which two statements apply to features of aggregate bandwidth allocation in Prisma Access for remote networks? (Choose two.)

A. Administrator can allocate up to 120% of the total bandwidth purchased for aggregate locations to support traffic peaks.

B. Administrator must assign a minimum of 50 MB to any compute location that will support remote networks.

C. Administrator is not required to allocate all purchased bandwidth to compute locations for the configuration to be valid.

D. Bandwidth that is allocated to a compute location is statically and evenly distributed across remote networks in that location.

Answer: A C

NO.51 Which connection method allows secure web gateway (SWG) access to internet-based SaaS applications using HTTP and HTTPS protocols?

A. GlobalProtect

B. Broker VM

C. explicit proxy

D. system-wide proxy

Answer: A

NO.52 What are two ways service connections and remote network connections differ? (Choose two.)

A. Remote network connections provide secondary WAN options, but service connections use backup service connection for redundancy.

B. Remote network connections enforce security policies, but service connections do not.

C. An on-premises resource cannot originate a connection to the internet over a service connection.

D. Service connections support both OSPF and BGP for routing protocols, but remote networks support only BGP.

Answer: A

NO.53 Which application gathers health telemetry about a device and its WiFi connectivity in order to help determine whether the device or the WiFi is the cause of any performance issues?

A. data loss prevention (DLP)

B. remote browser isolation (RBI)

C. Cortex Data Lake

D. GlobalProtect

Answer: C

NO.54 Organizations that require remote browser isolation (RBI) to protect their users can automate connectivity to third-party RBI products with which platform?

A. Zero Trust

B. SaaS Security API

C. GlobalProtect
D. CloudBlades API
Answer: A

NO.55 How does the secure access service edge (SASE) security model provide cost savings to organizations?
A. The single platform reduces costs compared to buying and managing multiple point products.
B. The compact size of the components involved reduces overhead costs, as less physical space is needed.
C. The content inspection integration allows third-party assessment, which reduces the cost of contract services.
D. The increased complexity of the model over previous products reduces IT team staffing costs.
Answer: C

NO.56 What allows enforcement of policies based on business intent, enables dynamic path selection, and provides visibility into performance and availability for applications and networks?
A. Identity Access Management (IAM) methods
B. Firewall as a Service (FWaaS)
C. Instant-On Network (ION) devices
D. Cloud Access Security Broker (CASB)
Answer: B

NO.57 What happens when SaaS Security sees a new or unknown SaaS application?
A. It forwards the application for WildFire analysis.
B. It uses machine learning (ML) to classify the application.
C. It generates alerts regarding changes in performance.
D. It extends the branch perimeter to the closest node with high performance.
Answer: A

NO.58 Which action protects against port scans from the internet?
A. Apply App-ID Security policy rules to block traffic sourcing from the untrust zone.
B. Assign Security profiles to Security policy rules for traffic sourcing from the untrust zone.
C. Apply a Zone Protection profile on the zone of the ingress interface.
D. Assign an Interface Management profile to the zone of the ingress surface.
Answer: C

NO.59 What is a key benefit of CloudBlades?
A. automation of UI workflow without any code development and deployment of Prisma SD-WAN ION devices
B. utilization of near real-time analysis to detect previously unseen, targeted malware and advanced persistent threats
C. identification of port-based rules so they can be converted to application-based rules without compromising application availability

D. configuration of the authentication source once instead of for each authentication method used

Answer: A

NO.60 Which element of Prisma Access enables both mobile users and users at branch networks to access resources in headquarters or a data center?

A. service connections

B. App-ID

C. private clouds

D. User-ID

Answer: A

NO.61 Users connect to a server in the data center for file sharing. The organization wants to decrypt the traffic to this server in order to scan the files being uploaded and downloaded to determine if malware or sensitive data is being moved by users.

Which proxy should be used to decrypt this traffic?

A. SCP Proxy

B. SSL Inbound Proxy

C. SSH Forward Proxy

D. SSL Forward Proxy

Answer: B

NO.62 Which App Response Time metric measures the amount of time it takes to transfer incoming data from an external server to a local client?

A. UDP Response Time (UDP-TRT)

B. Server Response Time (SRT)

C. Network Transfer Time (NTTn)

D. Round Trip Time (RTT)

Answer: D

NO.63 What is a benefit of the Palo Alto Networks secure access service edge (SASE) solution's ability to provide insight into SD-WAN and network security metrics while highlighting critical issues across all managed tenants?

A. It rearchitects the way signatures are delivered, performing updates and streaming them to the firewall within seconds after the analysis is done.

B. It helps protect inbound, outbound, and east-west traffic between container workload types in Kubernetes environments without slowing development speed.

C. It simplifies workflows and instantly automates common use cases with hundreds of prebuilt playbooks.

D. It helps managed service providers (MSPs) accelerate troubleshooting and meet service level agreements (SLAs) for all their customers.

Answer: D

NO.64 Which two prerequisites must an environment meet to onboard Prisma Access mobile users? (Choose two.)

A. Zoning must be configured to require a user ID for the mobile users trust zone.

B. Mapping of trust and untrust zones must be configured.

C. BGP must be configured so that service connection networks can be advertised to the mobile gateways.

D. Mobile user subnet and DNS portal name must be configured.

Answer: A D

NO.65 Which two actions take place after Prisma SD-WAN Instant-On Network (ION) devices have been deployed at a site? (Choose two.)

A. The devices continually sync the information from directories, whether they are on-premise, cloud-based, or hybrid.

B. The devices establish VPNs over private WAN circuits that share a common service provider.

C. The devices automatically establish a VPN to the data centers over every internet circuit.

D. The devices provide an abstraction layer between the Prisma SD-WAN controller and a particular cloud service.

Answer: A D

NO.66 What are two benefits of installing hardware fail-to-wire port pairs on Instant-On Network (ION) devices?
(Choose two.)

A. local area network (LAN) Dynamic Host Configuration Protocol (DHCP) and DHCP relay functionality

B. control mode insertion without modification of existing network configuration

C. network controller communication and monitoring

D. ensures automatic failover when ION devices experience software or network related failure

Answer: D

NO.67 Which three decryption methods are available in a security processing node (SPN)? (Choose three.)

A. SSL Outbound Proxy

B. SSHv2 Proxy

C. SSL Forward Proxy

D. SSL Inbound Inspection

E. SSH Inbound Inspection

Answer: B C D