ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which procedure is most effective for maintaining continuity and security during a Prisma Access data plane software upgrade?

A. Back up configurations, schedule upgrades during off-peak hours, and use a phased approach rather than attempting a network-wide rollout.

B. Use Strata Cloud Manager (SCM) to perform dynamic upgrades automatically and simultaneously across all locations at once to ensure network-wide uniformity.

C. Disable all security features during the upgrade to prevent conflicts and re-enable them after completion to ensure a smooth rollout process.

D. Perform the upgrade during peak business hours, quickly address any user-reported issues, and ensure immediate troubleshooting post-rollout.

Answer: A

Explanation:

The best practice for Prisma Access data plane upgrades involves backing up configurations, scheduling upgrades during off-peak hours, and using a phased approach to minimize disruption and maintain continuity. As per the Palo Alto Networks documentation:

"To minimize disruptions, it is recommended to perform Prisma Access upgrades during nonbusiness hours and in a phased manner, starting with less critical sites to validate the process before moving to critical locations. Backup configurations and validate the system's readiness to avoid data loss and maintain service continuity."

(Source: Prisma Access Best Practices)

Question: 2

An NGFW administrator is updating PAN-OS on company data center firewalls managed by Panoram

a. Prior to installing the update, what must the administrator verify to ensure the devices will continue to be supported by Panorama?

A. Device telemetry is enabled.

B. Panorama is configured as the primary device in the log collecting group for the data center firewalls.

C. All devices are in the same template stack.

D. Panorama is running the same or newer PAN-OS release as the one being installed.

Answer: D

Explanation:

The firewall must be running a PAN-OS version that is supported by Panorama. This means that Panorama must be running the same or a newer PAN-OS version as the one being installed on the firewalls to maintain compatibility.

"Before you upgrade the firewall, ensure that Panorama is running the same or a later PAN-OS version than the firewall. Panorama must always be at the same or a higher version to maintain compatibility."

(Source: Panorama Admin Guide – Upgrade Process)

Question: 3

In which two applications can Prisma Access threat logs for mobile user traffic be reviewed? (Choose two.)

A. Prisma Cloud dashboard

B. Strata Cloud Manager (SCM)

C. Strata Logging Service

D. Service connection firewall

Answer: B, C

Explanation:

Threat logs for Prisma Access mobile users can be reviewed in both Strata Cloud Manager (SCM) and Strata

Logging Service. Prisma Cloud and service connection firewalls are not directly tied to mobile user traffic logs.

"Prisma Access logs are available in the Strata Cloud Manager and can also be sent to the Strata Logging Service for detailed analysis and threat visibility."

(Source: Prisma Access Administration Guide)

Question: 4

Which two tools can be used to configure Cloud NGFWs for AWS? (Choose two.)

A. Cortex XSIAM

B. Prisma Cloud management console

C. Panorama

D. Cloud service provider's management console

Answer: C, D

Explanation:

Cloud NGFW for AWS can be configured using Panorama for centralized management, as well as the AWS management console for native integration and configuration.

"You can configure Cloud NGFW for AWS using Panorama for centralized security management, or directly through the AWS management console to deploy and manage security services for your AWS resources."

(Source: Cloud NGFW for AWS Guide)

Question: 5

Using Prisma Access, which solution provides the most security coverage of network protocols for the mobile workforce?

A. Explicit proxy
B. Client-based VPN
C. Enterprise browser
D. Clientless VPN

Answer: B

Explanation:

Client-based VPN solutions like GlobalProtect provide full coverage for the mobile workforce by extending the enterprise security stack to remote endpoints. It establishes a secure tunnel, allowing consistent security policies across the enterprise perimeter and the mobile workforce.

"GlobalProtect is a client-based VPN that provides secure, consistent protection for mobile users by extending the security capabilities of Prisma Access to remote endpoints, covering all network protocols."

(Source: GlobalProtect Admin Guide)

Question: 6

Which two prerequisites must be evaluated when decrypting internet-bound traffic? (Choose two.)

A. RADIUS profile
B. Incomplete certificate chains
C. Certificate pinning
D. SAML certificate

Answer: B, C

Explanation:

When implementing SSL Forward Proxy decryption for outbound traffic, two key challenges that must be evaluated are:

Incomplete certificate chains: This occurs when the firewall cannot validate the entire certificate chain for a site, which may cause decryption failures.

Certificate pinning: Applications like banking apps may use certificate pinning to prevent MITM (man-in-the-

middle) attacks, and these applications will break if SSL Forward Proxy is used.
"When decrypting outbound SSL traffic, you must consider incomplete certificate chains, which can cause decryption to fail if the firewall cannot validate the entire chain. Also, be aware of certificate pinning in applications that prevents decryption by rejecting forged certificates."
(Source: Palo Alto Networks Decryption Concepts)

Question: 7

Which firewall attribute can an engineer use to simplify rule creation and automatically adapt to changes in server roles or security posture based on log events?

A. Address objects
B. Dynamic Address Groups
C. Dynamic User Groups
D. Predefined IP addresses

Answer: B

Explanation:

Dynamic Address Groups enable the firewall to automatically adjust security policies based on tags assigned dynamically (via log events, API, etc.). This eliminates the need for manual updates to policies when server roles or IPs change.
"Dynamic Address Groups allow you to create policies that automatically adapt to changes in the environment. These groups are populated dynamically based on tags, enabling automated security policy updates without manual intervention."
(Source: Dynamic Address Groups)

Question: 8

How does a firewall behave when SSL Inbound Inspection is enabled?

A. It acts transparently between the client and the internal server.

B. It decrypts inbound and outbound SSH connections.

C. It decrypts traffic between the client and the external server.

D. It acts as meddler-in-the-middle between the client and the internal server.

Answer: D

Explanation:

SSL Inbound Inspection allows the firewall to decrypt incoming encrypted traffic to internal servers (e.g., web servers) by acting as a man-in-the-middle (MITM). The firewall uses the private key of the server to decrypt the session and apply security policies before re-encrypting the traffic.

"SSL Inbound Inspection requires you to import the server's private key and certificate into the firewall. The firewall then acts as a man-in-the-middle (MITM) to decrypt inbound sessions from external clients to internal servers for inspection."

(Source: SSL Inbound Inspection)

Question: 9

When a firewall acts as an application-level gateway (ALG), what does it require in order to establish a connection?

A. Dynamic IP and Port (DIPP)

B. Payload

C. Session Initiation Protocol (SIP)

D. Pinholes

Answer: B

Explanation:

An ALG is designed to inspect and modify the payload of application-layer protocols (like SIP, FTP, etc.) to manage dynamic port allocations and session information.

"Application Layer Gateways (ALGs) inspect the payload of certain protocols to dynamically manage sessions that use dynamic port assignments. By modifying payloads, the ALG ensures that NAT and security policies are correctly applied."

(Source: ALG Support)

Question: 10

Which security profile provides real-time protection against threat actors who exploit the misconfigurations of DNS infrastructure and redirect traffic to malicious domains?

A. Antivirus
B. URL Filtering
C. Vulnerability Protection
D. Anti-spyware

Answer: D

Explanation:

The Anti-spyware profile includes DNS-based protections like sinkholing and detection of DNS queries to malicious domains, offering real-time protection against attacks that exploit DNS misconfigurations.

"The Anti-Spyware profile protects against DNS-based threats by sinkholing DNS queries to malicious domains and detecting suspicious DNS activity, thus blocking data exfiltration and C2 communication."

(Source: Anti-Spyware Profiles)

Question: 11

Which method in the WildFire analysis report detonates unknown submissions to provide visibility into real-world effects and behavior?

A. Dynamic analysis

B. Static analysis

C. Intelligent Run-time Memory Analysis

D. Machine learning (ML)

Answer: A

Explanation:

Dynamic analysis in WildFire refers to executing unknown files in a controlled environment (sandbox) to observe their real-world behavior. This allows the firewall to detect zero-day threats and advanced malware by directly analyzing the file's impact on a system.

"WildFire dynamic analysis detonates unknown files in a secure sandbox environment, analyzing real-world effects, behaviors, and potential malicious activity."

(Source: WildFire Analysis)

Question: 12

How many places will a firewall administrator need to create and configure a custom data loss prevention (DLP) profile across Prisma Access and the NGFW?

A. One

B. Two

C. Three

D. Four

Answer: A

Explanation:

Palo Alto Networks' Enterprise DLP uses a centralized DLP profile that can be applied consistently across both Prisma Access and NGFWs using Strata Cloud Manager (SCM). This eliminates the need for duplicating efforts across multiple locations.

"Enterprise DLP profiles are created and managed centrally through the Cloud Management Interface and can be used seamlessly across NGFW and Prisma Access deployments."

(Source: Enterprise DLP Overview)

Question: 13

A cloud security architect is designing a certificate management strategy for Strata Cloud Manager (SCM) across hybrid environments. Which practice ensures optimal security with low management overhead?

A. Deploy centralized certificate automation with standardized protocols and continuous monitoring.

B. Implement separate certificate authorities with independent validation rules for each cloud environment.

C. Configure manual certificate deployment with quarterly reviews and environment-specific security protocols.

D. Use cloud provider default certificates with scheduled synchronization and localized renewal processes.

Answer: A

Explanation:

A centralized certificate automation approach reduces management overhead and security risks by standardizing processes, automating renewals, and continuously monitoring the certificate lifecycle.

"Implementing a centralized certificate management approach with automation and continuous monitoring ensures optimal security while reducing operational complexity in hybrid environments."

(Source: Best Practices for Certificate Management)

Question: 14

Which set of practices should be implemented with Cloud Access Security Broker (CASB) to ensure robust data encryption and protect sensitive information in SaaS applications?

A. Do not enable encryption for data-at-rest to improve performance.

B. Use default encryption keys provided by the SaaS provider.

C. Perform annual encryption key rotations.

D. Enable encryption for data-at-rest and in transit, regularly update encryption keys, and use strong encryption algorithms.

Answer: D

Explanation:

CASB integration should focus on comprehensive data protection, which includes encryption for data-at-rest and in transit, frequent key updates, and using strong encryption algorithms to ensure confidentiality and

data integrity.

"CASB solutions should enforce encryption for data-at-rest and in transit, implement key rotation policies, and leverage robust encryption algorithms to protect sensitive SaaS application data."

(Source: CASB Deployment Best Practices)

Question: 15

How does Strata Logging Service help resolve ever-increasing log retention needs for a company using Prisma Access?

A. It increases resilience due to decentralized collection and storage of logs.

B. Automatic selection of physical data storage regions decreases adoption time.

C. It can scale to meet the capacity needs of new locations as business grows.

D. Log traffic using the licensed bandwidth purchased for Prisma Access reduces overhead.

Answer: C

Explanation:

The Strata Logging Service offers scalable log storage to accommodate data growth, which ensures organizations can retain logs for compliance and threat hunting as their environments expand.

"The Strata Logging Service is designed to scale dynamically to accommodate growing log retention needs, allowing enterprises to maintain comprehensive visibility as they expand their network footprint."

(Source: Strata Logging Service Overview)

Question: 16

After a firewall is associated with Strata Cloud Manager (SCM), which two additional actions are required to enable management of the firewall from SCM? (Choose two.)

A. Deploy a service connection for each branch site and connect with SCM.

B. Configure NTP and DNS servers for the firewall.

C. Configure a Security policy allowing “stratacloudmanager.paloaltonetworks.com” for all users.

D. Install a device certificate.

Answer: B, D

Explanation:

To fully manage a firewall from Strata Cloud Manager (SCM), it’s essential to establish trust and ensure reliable connectivity:

Configure NTP and DNS servers

The firewall must have accurate time (NTP) and name resolution (DNS) to securely communicate with SCM and related cloud services.

“To ensure successful management, configure the firewall’s NTP and DNS settings to synchronize time and resolve domain names such as stratacloudmanager.paloaltonetworks.com.”

(Source: SCM Onboarding Requirements)

Install a device certificate

A device certificate authenticates the firewall’s identity when connecting to SCM.

“The device certificate authenticates the firewall to Palo Alto Networks cloud services, including SCM. It’s a fundamental requirement to establish secure connectivity.”

(Source: Device Certificates)

These steps ensure trust, secure communication, and successful onboarding into SCM.

Question: 17

How does Advanced WildFire integrate into third-party applications?

A. Through playbooks automatically sending WildFire data

B. Through customized reporting configured in NGFWs

C. Through Strata Logging Service

D. Through the WildFire API

Answer: D

Explanation:

Advanced WildFire supports direct integrations into third-party security tools through the WildFire API, enabling automated threat intelligence sharing and real-time verdict dissemination.

"WildFire exposes a RESTful API that third-party applications can leverage to integrate WildFire's analysis results and threat intelligence seamlessly into their own security workflows."
(Source: WildFire API Guide)

The API provides:

Verdict retrieval

Sample submission

Report retrieval

"Use the WildFire API to submit samples, retrieve verdicts, and obtain detailed analysis reports for integration with your existing security infrastructure."
(Source: WildFire API Use Cases)

Question: 18

Which two SSH Proxy decryption profile settings should be configured to enhance the company's security posture? (Choose two.)

A. Block sessions when certificate validation fails.

B. Allow sessions with legacy SSH protocol versions.

C. Block connections that use non-compliant SSH versions.

D. Allow sessions when decryption resources are unavailable.

Answer: A, C

Explanation:

Blocking non-compliant SSH versions and failing certificate validations are fundamental security measures:

Block sessions when certificate validation fails

"The SSH Proxy profile should block sessions that fail certificate validation to ensure that only trusted hosts are allowed."

(Source: SSH Proxy Decryption Best Practices)

Block connections using non-compliant SSH versions

Older SSH versions may have vulnerabilities or lack modern encryption algorithms.

"To enforce stronger security, block SSH sessions that use older or deprecated versions of the SSH protocol that do not comply with your security posture."

(Source: SSH Decryption and Best Practices)

Together, these measures minimize the risk of MITM attacks and secure SSH traffic.

Question: 19

A network security engineer has created a Security policy in Prisma Access that includes a negated region in the source address. Which configuration will ensure there is no connectivity loss due to the negated region?

A. Set the service to be application-default.

B. Create a Security policy for the negated region with destination address “any”.

C. Add a Dynamic Application Group to the Security policy.

D. Add all regions that contain private IP addresses to the source address.

Answer: B

Explanation:

Negated source addresses exclude traffic from the specified region. To avoid accidental connectivity loss for traffic from that region, create a separate Security policy to explicitly permit it.

“When you use a negated region in a Security policy rule, ensure to create an additional Security policy to permit traffic from the excluded (negated) region to avoid unintentional drops.”

(Source: Prisma Access Policy Best Practices)

This ensures explicit inclusivity for the excluded region, maintaining reliable connectivity.

Question: 20

What is a necessary step for creation of a custom Prisma Access report on Strata Cloud Manager (SCM)?

A. Open a support ticket.

B. Set up Cloud Identity Engine.

C. Generate a PDF summary report.

D. Configure a dashboard.

Answer: D

Explanation:

To create custom Prisma Access reports within SCM, you first configure a dashboard that aggregates the relevant logs and analytics. This allows you to define the data points you want to include.

"Dashboards in SCM can be customized to include Prisma Access data sources, enabling you to create and generate reports that meet specific business and security requirements."

(Source: SCM Dashboards and Reporting)

Once configured, you can export the dashboard as a custom report.

"Use the dashboard's data visualization to create custom reports for Prisma Access, which can be exported as PDFs for distribution."

(Source: SCM Report Customization)

Question: 21

Which NGFW function can be used to enhance visibility, protect, block, and log the use of Postquantum Cryptography (PQC)?

A. DNS Security profile

B. Decryption policy

C. Security policy

D. Decryption profile

Answer: B

Explanation:

A decryption policy allows the firewall to inspect encrypted traffic and apply security controls to Postquantum Cryptography (PQC) usage, as PQC algorithms are typically implemented within encrypted sessions.

"Decryption policies enable the firewall to see and control encrypted traffic. This visibility and control extend to new cryptographic algorithms, including PQC, to ensure that security measures are applied consistently."

(Source: Palo Alto Networks Decryption Overview)

By decrypting sessions, you ensure that even PQC traffic can be inspected, logged, and subject to security profiles for visibility and policy enforcement.

Question: 22

What is the recommended upgrade path from PAN-OS 9.1 to PAN-OS 11.2?

A. 9.1 → 11.0 → 11.2

B. 9.1 → 10.0 → 11.

C. 9.1 → 11.

D. 9.1 → 10.0 → 11.2

Answer: D

Explanation:

Palo Alto Networks requires upgrading to the next major feature release before moving to newer releases. This ensures stability and compatibility.

"When upgrading across multiple major PAN-OS releases, you must upgrade to each intermediate major feature release. Skipping major releases is not supported."

(Source: Upgrade Considerations)

For PAN-OS 9.1 → 11.2, the proper path is:

9.1 → 10.0 → 11.2

Question: 23

Which two features can a network administrator use to troubleshoot the issue of a Prisma Access mobile user who is unable to access SaaS applications? (Choose two.)

A. SaaS Application Risk Portal

B. Capacity Analyzer

C. GlobalProtect logs

D. Autonomous Digital Experience Manager (ADEM) console

Answer: C, D

Explanation:

GlobalProtect logs

These logs provide detailed insights into the user's connectivity, tunnel status, and authentication events.

"GlobalProtect logs include detailed information about connection establishment, tunnel negotiation, and any errors that can prevent mobile users from accessing applications."

(Source: GlobalProtect Troubleshooting)

Autonomous Digital Experience Management (ADEM)

ADEM helps visualize end-to-end performance and identifies network issues affecting SaaS app access for mobile users.

"ADEM provides real-time and historical visibility into user experience, enabling quick identification and resolution of connectivity or performance issues for SaaS applications."

(Source: ADEM for Prisma Access)

Question: 24

Which two content updates can be pushed to next-generation firewalls from Panorama? (Choose two.)

A. Advanced URL Filtering

B. Applications and threats

C. WildFire

D. GlobalProtect data file

Answer: B, C

Explanation:

Applications and threats

Panorama can push application and threat signature updates to managed firewalls, ensuring consistent application and threat visibility.

"Panorama uses dynamic updates to distribute the latest application and threat signature packs to all managed firewalls."

(Source: Manage Content Updates in Panorama)

WildFire

Panorama also distributes WildFire signature updates to firewalls for real-time malware detection.

"WildFire updates provide the latest malware signatures to enhance detection and prevention, and can be deployed to all managed firewalls via Panorama."

(Source: WildFire and Dynamic Updates)

Question: 25

A network administrator obtains Palo Alto Networks Advanced Threat Prevention and Advanced DNS Security subscriptions for edge NGFWs and is setting up security profiles. Which step should be included in the initial configuration of the Advanced DNS Security service?

A. Create a decryption policy rule to decrypt DNS-over-TLS / port 853 traffic.

B. Create overrides for all company owned FQDNs.

C. Configure DNS Security signature policy settings to sinkhole malicious DNS queries.

D. Enable Advanced Threat Prevention with default settings and only focus on high-risk traffic.

Answer: C

Explanation:

Advanced DNS Security uses a signature policy to sinkhole malicious DNS queries and prevent them from resolving.

"The DNS Security service integrates with Anti-Spyware profiles, and you must configure signature policy settings to sinkhole malicious queries. This proactively stops traffic to known malicious domains."

(Source: Configure DNS Security)

Sinkholing ensures that DNS queries to malicious FQDNs are redirected to a safe IP, preventing compromise.

Question: 26

What must be configured to successfully onboard a Prisma Access remote network using Strata Cloud Manager (SCM)?

A. Cloud Identity Engine
B. Autonomous Digital Experience Manager (ADEM)
C. GlobalProtect agent
D. IPSec termination node

Answer: D

Explanation:

To connect a remote network to Prisma Access via Strata Cloud Manager (SCM), the remote network requires an IPSec termination node. This acts as the VPN endpoint, ensuring secure connectivity between branch locations and Prisma Access.

"To onboard a remote network, configure the IPSec termination node on the customer's premises. This VPN endpoint establishes the secure tunnel to Prisma Access for traffic backhauling."

(Source: Onboard Remote Networks)

Key takeaway:

The IPSec termination node is fundamental for secure, encrypted connectivity.

Question: 27

In a Prisma SD-WAN environment experiencing voice quality degradation, which initial action is recommended?

A. Immediately modify path quality thresholds.
B. Review real-time analytics of path performance.
C. Switch all VoIP traffic to backup paths.
D. Request an RMA of the ION devices.

Answer: B

Explanation:

Voice quality issues in SD-WAN deployments are typically linked to path performance metrics (latency, jitter, packet loss). Reviewing real-time analytics helps pinpoint root causes and appropriate mitigation.

"When experiencing performance issues, the first step is to analyze real-time performance data. Prisma SD-WAN provides path quality analytics to identify degradation and ensure informed troubleshooting."

(Source: Prisma SD-WAN Monitoring)

This data-driven approach avoids unnecessary configuration changes.

Question: 28

Which action optimizes user experience across a segmented network architecture and implements the most effective method to maintain secure connectivity between branch and campus locations?

A. Establish site-to-site tunnels on each branch and campus firewall and have individual VLANs for each department.

B. Configure all branch and campus firewalls to use a single shared broadcast domain.

C. Implement SD-WAN to route all traffic based on network performance metrics and use zone protection profiles.

D. Configure a single campus firewall to handle the routing of all branch traffic.

Answer: C

Explanation:

SD-WAN solutions optimize application experience and provide secure, dynamic connectivity across distributed locations by leveraging real-time path metrics (latency, jitter, loss).

"By implementing SD-WAN, traffic is routed intelligently based on real-time network performance metrics. Zone protection profiles ensure security while maximizing application performance."
(Source: SD-WAN Architecture)

Key advantage:

Secure connectivity and best user experience across campuses and branches.

Question: 29

When configuring Security policies on VM-Series firewalls, which set of actions will ensure the most comprehensive Security policy enforcement?

A. Configure port-based policies, check threat logs weekly, conduct software updates annually, and enable decryption.

B. Configure policies using User-ID and App-ID, enable decryption, apply appropriate security profiles to rules, and update regularly with dynamic updates.

C. Configure all default policies provided by the firewall, use Policy Optimizer, and adjust security rules after an incident occurs.

D. Configure a block policy for all malicious inbound traffic, configure an allow policy for all outbound traffic,

and update regularly with dynamic updates.

Answer: B

Explanation:

A comprehensive security approach uses:

User-ID for identity-based policies

App-ID for application-based security

Decryption to inspect encrypted traffic

Security profiles to enforce protections

Dynamic updates to ensure up-to-date threat coverage

"For comprehensive security, combine User-ID, App-ID, decryption, and security profiles. Keep the firewall updated with dynamic content updates to maintain the strongest security posture."

(Source: Best Practices for Security Policy)

This ensures real-time, identity-aware, and application-centric security enforcement.

Question: 30

Which functionality does an NGFW use to determine whether new session setups are legitimate or illegitimate?

A. SYN bit

B. SYN cookies

C. Random Early Detection (RED)

D. SYN flood protection

Answer: B

Explanation:

To prevent SYN flood attacks, the NGFW uses SYN cookies to validate legitimate session establishment.

"SYN cookies allow the firewall to verify the legitimacy of new session requests without allocating resources until the handshake is completed. This prevents SYN flood attacks from exhausting system resources."

(Source: Flood Protection Best Practices)

SYN cookies mitigate resource exhaustion by ensuring only legitimate connections are established.

Question: 31

Which two security services are required for configuration of NGFW Security policies to protect against malicious and misconfigured domains? (Choose two.)

A. Advanced Threat Prevention
B. SaaS Security
C. Advanced WildFire
D. Advanced DNS Security

Answer: A, D

Explanation:

Protecting against malicious and misconfigured domains requires two critical services:

Advanced Threat Prevention

Provides signature-based and advanced analysis to identify threats, including DNS-based attacks.

"Advanced Threat Prevention enables the NGFW to detect and prevent exploits and malware-based communications, including those leveraging DNS."

(Source: Advanced Threat Prevention)

Advanced DNS Security

Specifically designed to detect and sinkhole malicious and misconfigured DNS queries.

"DNS Security uses real-time intelligence to block DNS-based threats, protect against data exfiltration, and automatically sinkhole suspicious domain lookups."

(Source: DNS Security)

By combining these services in security policies, NGFWs ensure robust protection against domain-based threats and misconfigurations.

Question: 32

Which step is necessary to ensure an organization is using the inline cloud analysis features in its Advanced Threat Prevention subscription?

A. Disable anti-spyware to avoid performance impacts and rely solely on external threat intelligence.

B. Enable SSL decryption in Security policies to inspect and analyze encrypted traffic for threats.

C. Update or create a new anti-spyware security profile and enable the appropriate local deep learning models.

D. Configure Advanced Threat Prevention profiles with default settings and only focus on high-risk traffic to avoid affecting network performance.

Answer: C

Explanation:

To fully leverage inline cloud analysis in Advanced Threat Prevention, security profiles (e.g., antispyware) must be updated or newly created to enable local deep learning and inline cloud analysis models.

"To activate inline cloud analysis, update your Anti-Spyware profile to enable advanced inline detection engines, including deep learning-based models and cloud-delivered signatures."

(Source: Inline Cloud Analysis and Deep Learning)

This ensures real-time protection from sophisticated threats beyond static signatures.

Question: 33

Which zone is available for use in Prisma Access?

A. Clientless VPN

B. Interzone

C. Intrazone

D. DMZ

Answer: B

Explanation:

In Prisma Access, the interzone security policy rule is available and plays a crucial role in controlling traffic between zones.

"You can configure an interzone rule to control traffic that flows between different zones in Prisma Access, enabling granular security policy enforcement."

(Source: Prisma Access Security Policies)

This ensures comprehensive control of traffic crossing security boundaries in the cloud-delivered architecture.

Question: 34

Which offering can be managed in both Panorama and Strata Cloud Manager (SCM)?

A. Autonomous Digital Experience Manager (ADEM)

B. VM-Series Next-Generation Firewall (NGFW)

C. Prisma SD-WAN

D. SaaS Security

Answer: B

Explanation:

The VM-Series NGFWs are designed to integrate seamlessly with both Panorama and Strata Cloud Manager (SCM), allowing administrators to manage physical and virtual firewall deployments from either interface.

"You can manage VM-Series Next-Generation Firewalls using either Panorama for centralized management of all firewalls or Strata Cloud Manager for cloud-based management, giving flexibility across hybrid environments."

(Source: VM-Series Management Options)

Unified management flexibility is key for enterprises with hybrid or multi-cloud deployments.

Question: 35

Which component of NGFW is supported in active/passive design but not in active/active design?

A. Single floating IP address

B. Using a DHCP client

C. Route-based redundancy

D. Configuring ARP load-sharing on Layer 3

Answer: A

Explanation:

Single floating IP address (also known as a floating IP or shared IP) is supported only in an active/passive HA pair. In active/active HA, both firewalls are forwarding traffic simultaneously and thus do not share a single floating IP.

"In active/passive HA, a single floating IP address is used for seamless failover. Active/active HA requires separate IP addresses and does not support a single floating IP."

(Source: Active/Passive vs. Active/Active HA)

This simplifies failover in active/passive deployments by using a single shared IP that moves to the active peer upon failover.

Question: 36

What key capability distinguishes Content-ID technology from conventional network security approaches?

A. It performs packet header analysis short of deep packet inspection.

B. It provides single-pass application layer inspection for real-time threat prevention.

C. It exclusively monitors network traffic volumes.

D. It relies primarily on reputation-based filtering.

Answer: B

Explanation:

Content-ID is the core of Palo Alto Networks' prevention architecture, providing single-pass application layer inspection to deliver real-time threat prevention across all traffic.

"Content-ID uses a single-pass architecture to perform application-layer (Layer 7) traffic inspection

and real-time threat prevention. Unlike traditional firewalls that rely on multiple scans, Content-ID inspects traffic once to enforce multiple security controls simultaneously."

(Source: Content-ID Overview)

By consolidating security functions in a single pass, it ensures both efficiency and comprehensive security.

Question: 37

In a distributed enterprise implementing Prisma SD-WAN, which configuration element should be implemented first to ensure optimal traffic flow between remote sites and headquarters?

A. Deploy redundant ION devices at each location.

B. Implement dynamic path selection using real-time performance metrics.

C. Configure static routes between all the branch offices.

D. Enable split tunneling for all branch locations.

Answer: B

Explanation:

Dynamic path selection is the foundation of SD-WAN, leveraging real-time performance data to dynamically route traffic over the best available path.

"Dynamic path selection continuously monitors performance metrics (loss, latency, jitter) and makes real-time routing decisions to ensure application SLAs are met across the WAN."

(Source: Prisma SD-WAN Dynamic Path Selection)

Establishing dynamic path selection first ensures the rest of the SD-WAN optimizations (e.g., failover, QoS) work effectively.

Question: 38

Which two components of a Security policy, when configured, allow third-party contractors access to internal applications outside business hours? (Choose two.)

A. App-ID

B. Service

C. User-ID

D. Schedule

Answer: C, D

Explanation:

To allow third-party contractors controlled access, security policies must combine user identification and time-based access controls:

User-ID

"User-ID enables security policies to be based on user identity rather than IP addresses, ensuring precise policy enforcement for specific users such as contractors."

(Source: User-ID Overview)

Schedule

"Schedules allow policies to be active only during specific times, providing time-based access control (e.g., after business hours)."

(Source: Security Policy Schedules)

Together, they ensure that only authorized users (contractors) have access, and only when explicitly allowed.

Question: 39

A company has an ongoing initiative to monitor and control IT-sanctioned SaaS applications. To be successful, it

will require configuration of decryption policies, along with data filtering and URL Filtering Profiles used in Security policies. Based on the need to decrypt SaaS applications, which two steps are appropriate to ensure success? (Choose two.)

A. Configure SSL Forward Proxy.

B. Validate which certificates will be used to establish trust.

C. Configure SSL Inbound Inspection.

D. Create new self-signed certificates to use for decryption.

Answer: A, B

Explanation:

To inspect SaaS app traffic (often encrypted), you must configure:

SSL Forward Proxy

"The SSL Forward Proxy decryption profile enables the firewall to decrypt outbound SSL traffic, essential for visibility into SaaS app usage."

(Source: SSL Forward Proxy Overview)

Validate certificates

"Validating and deploying the appropriate root and intermediate CA certificates is critical for establishing trust and preventing SSL errors during decryption."

(Source: Certificate Deployment and Validation)

Without these steps, SaaS decryption and policy enforcement would be incomplete.

Question: 40

A network security engineer wants to forward Strata Logging Service data to tools used by the Security Operations Center (SOC) for further investigation. In which best practice step of Palo Alto Networks Zero Trust does this fit?

A. Map and Verify Transactions

B. Implementation

C. Standards and Designs

D. Report and Maintenance

Answer: D

Explanation:

The “Report and Maintenance” step of the Zero Trust model emphasizes ongoing monitoring, analysis, and reporting to ensure the environment remains secure over time.

“The Report and Maintenance phase includes continuous monitoring, log forwarding, and sharing of security telemetry to third-party tools to maintain and validate Zero Trust implementation.”

(Source: Zero Trust Best Practices)

By forwarding logs to SOC tools, the engineer ensures comprehensive visibility and proactive threat hunting.

Question: 41

A network engineer pushes specific Panorama reports of new AI URL category types to branch NGFWs. Which two report types achieve this goal? (Choose two.)

A. SNMP

B. Custom

C. PDF summary

D. CSV export

Answer: B, C

Explanation:

Panorama allows engineers to create custom reports and generate PDF summary formats for consistent reporting across NGFWs.

Custom Reports

"Custom Reports provide tailored reporting based on URL categories, application usage, and threat visibility. They are generated within Panorama and can include data on newly categorized AI URL types."

(Source: Panorama Reports)

PDF Summaries

"You can generate PDF summary reports to distribute these insights across branch firewalls, providing an easy-to-read format for compliance and operational review."

(Source: Export Reports as PDF)

Together, these options provide a consistent, standardized method to push insights about AI-based URL categories to branch devices.

Question: 42

Which subscription sends non-file format-based traffic that matches Data Filtering Profile criteria to a cloud service to render a verdict?

A. Enterprise DLP

B. Advanced URL Filtering

C. SaaS Security Inline

D. Advanced WildFire

Answer: A

Explanation:

Enterprise DLP uses cloud analysis to inspect and classify sensitive data in non-file-based formats (e.g., in-line data streams, SaaS communications).

"Enterprise DLP inspects data in non-file-based traffic flows, forwarding suspicious data patterns to the cloud for classification and verdicts."

(Source: Enterprise DLP Overview)

The other services focus on file-based scanning (WildFire), URL access control (Advanced URL Filtering), or inline SaaS application controls (SaaS Security Inline).

Question: 43

How are policies evaluated in the AWS management console when creating a Security policy for a Cloud NGFW?

A. The administrator sets a rule order to determine the order in which they are evaluated.

B. They can be dragged up or down the stack as they are evaluated.

C. The administrator sets a rule priority to determine the order in which they are evaluated.

D. They must be created in the order they are intended to be evaluated.

Answer: D

Explanation:

Cloud NGFW Security Policies in the AWS Console are evaluated in the exact creation order – they do not have explicit rule priority fields.

"In AWS, security rules are evaluated in the order they are created. To ensure the correct evaluation logic, create them in the desired order from top to bottom."

(Source: Cloud NGFW for AWS Policy Evaluation)

Unlike Panorama, AWS-native management of Cloud NGFWs uses creation order as the evaluation sequence.

Question: 44

During a security incident investigation, which Security profile will have logs of attempted confidential data exfiltration?

A. File Blocking Profile

B. Enterprise DLP Profile

C. Vulnerability Protection Profile

D. WildFire Analysis Profile

Answer: B

Explanation:

Enterprise DLP Profile is specifically designed to detect and log data exfiltration attempts, including those involving confidential or sensitive data.

"Enterprise DLP logs capture incidents involving potential data exfiltration. They help identify sensitive data transfers, even in seemingly legitimate traffic."

(Source: Enterprise DLP Logging and Alerts)

File Blocking and Vulnerability Protection handle files or exploit detection, while WildFire focuses on malware analysis—not direct data exfiltration.

Question: 45

Which set of attributes is used by IoT Security to identify and classify appliances on a network when determining Device-ID?

A. IP address, network traffic patterns, and device type

B. MAC address, device manufacturer, and operating system

C. Hostname, application usage, and encryption method

D. Device model, firmware version, and user credential

Answer: B

Explanation:

IoT Security uses MAC address, device manufacturer, and OS information to identify and classify devices via Device-ID.

"IoT Security uses passive network traffic analysis to fingerprint devices based on the MAC address, manufacturer, and operating system to ensure accurate classification."

(Source: IoT Security Device-ID and Classification)

These attributes provide a robust, manufacturer-agnostic method to fingerprint IoT devices.

Question: 46

Which two types of logs must be forwarded to Strata Logging Service for IoT Security to function? (Choose two.)

A. WildFire

B. Enhanced application

C. Threat

D. URL Filtering

Answer: B, C

Explanation:

For IoT Security to accurately classify and monitor IoT devices, the following logs must be forwarded to Strata Logging Service:

Enhanced application logs – provide detailed application usage and behaviors, essential for profiling device types and roles.

"Enhanced Application logs provide additional context on IoT device behavior and usage patterns, and must be forwarded to Strata Logging Service for IoT Security to build accurate Device-ID profiles."

(Source: IoT Security Logging Requirements)

Threat logs – essential for detecting suspicious or malicious activities by IoT devices.

"Threat logs are critical for identifying potential exploits or suspicious activities involving IoT devices and are required for accurate threat visibility within IoT Security."

(Source: IoT Security Logs)

These logs collectively ensure accurate device classification and real-time threat visibility.

Question: 47

Which action is only taken during slow path in the NGFW policy?

A. Session lookup

B. Layer 2—Layer 4 firewall processing

C. SSL/TLS decryption

D. Security policy lookup

Answer: C

Explanation:

In Palo Alto Networks' Single-Pass Parallel Processing (SP3) architecture, SSL/TLS decryption occurs only during the slow path when the firewall first encounters a new session.

"SSL/TLS decryption, which requires CPU-intensive cryptographic operations, is performed during the slow path when establishing new sessions. Once decrypted, traffic is processed in the fast path for subsequent packets."

(Source: Packet Flow and SP3 Architecture)

After the initial decryption in the slow path, decrypted traffic is handled by fast path for efficiency.

Question: 48

Which feature of SaaS Security will allow a firewall administrator to identify unknown SaaS applications in an environment?

A. App-ID Cloud Engine
B. App-ID
C. SaaS Data Security
D. Cloud Identity Engine

Answer: A

Explanation:

App-ID Cloud Engine (ACE) in SaaS Security uses cloud-based signatures to detect unknown and unsanctioned SaaS applications in the environment.

“App-ID Cloud Engine (ACE) uses real-time cloud intelligence to identify SaaS applications, including previously unknown or newly introduced applications.”

(Source: ACE for SaaS Visibility)

This feature is key for comprehensive SaaS visibility beyond static signatures.

Question: 49

How do Cloud NGFW instances get created when using AWS centralized deployments?

A. Cloud NGFW is placed in a vWAN with a virtual hub.
B. They replace the internet gateway service.
C. Selected VPCs will have Cloud NGFW workloads added to them.
D. A security VPC will be created as transit gateways to push all traffic through the area.

Answer: C

Explanation:

When using AWS centralized deployments for Cloud NGFW, the service deploys NGFW instances into selected VPCs as additional workloads to secure that traffic.

"In centralized deployments, Cloud NGFW instances are deployed as security appliances within the selected VPCs, ensuring consistent traffic inspection and protection."

(Source: Cloud NGFW Deployment Models)

This approach minimizes complexity and ensures direct security policy enforcement within AWS.

Question: 50

Which GlobalProtect configuration is recommended for granular security enforcement of remote user device posture?

A. Configuring host information profile (HIP) checks for all mobile users

B. Configuring a rule that blocks the ability of users to disable GlobalProtect while accessing internal applications

C. Implementing multi-factor authentication (MFA) for all users attempting to access internal applications

D. Applying log at session end to all GlobalProtect Security policies

Answer: A

Explanation:

Host Information Profile (HIP) checks are used in GlobalProtect to collect and evaluate endpoint posture (OS, patch level, AV status) to enforce granular security policies for remote users.

"The HIP feature collects information about the host and can be used in security policies to enforce posture-

based access control. This ensures only compliant endpoints can access sensitive resources."

(Source: GlobalProtect HIP Checks)

This enables fine-grained, context-aware access decisions beyond user identity alone.

Question: 51

Which AI-powered solution provides unified management and operations for NGFWs and Prisma Access?

A. Strata Cloud Manager (SCM)

B. Autonomous Digital Experience Manager (ADEM)

C. Prisma Access Browser

D. Panorama

Answer: A

Explanation:

Strata Cloud Manager (SCM) offers a cloud-based unified management plane for both NGFWs and Prisma Access, enabling consistent policy enforcement, simplified management, and AI-driven operational insights.

"Strata Cloud Manager provides a single interface for unified management of NGFWs and Prisma Access, leveraging AI to optimize security operations and streamline workflows."

(Source: Strata Cloud Manager Overview)

Unlike Panorama, which is an on-premises management solution, SCM delivers cloud-based, AIdriven capabilities for centralized oversight.

Question: 52

Which action allows an engineer to collectively update VM-Series firewalls with Strata Cloud Manager (SCM)?

A. Creating an update grouping rule

B. Scheduling software update

C. Creating a device grouping rule

D. Setting a target OS version

Answer: C

Explanation:

Device grouping rules in SCM allow administrators to organize firewalls into logical groups and collectively manage updates or configuration pushes across those groups.

"SCM allows you to create device group rules, enabling streamlined management and collective updates of multiple NGFW instances."

(Source: SCM Device Grouping)

This approach ensures consistency in software versions and configuration baselines across large deployments.

Question: 53

A network security engineer needs to implement segmentation but is under strict compliance requirements to place security enforcement as close as possible to the private applications hosted in Azure. Which deployment style is valid and meets the requirements in this scenario?

A. On a VM-Series NGFW, configure several Layer 2 zones with Layer 2 interfaces assigned to logically

segment the network.

B. On a PA-Series NGFW, configure several Layer 2 zones with Layer 2 interfaces assigned to logically segment the network.

C. On a VM-Series NGFW, configure several Layer 3 zones with Layer 3 interfaces assigned to logically segment the network.

D. On a PA-Series NGFW, configure several Layer 3 zones with Layer 3 interfaces assigned to logically segment the network.

Answer: C

Explanation:

In cloud environments like Azure, the VM-Series NGFW is deployed to create Layer 3 segmentation zones closest to the application workloads.

"In Azure, deploy VM-Series firewalls in Layer 3 mode to enforce security policies closest to private applications, meeting strict compliance and segmentation requirements."

(Source: VM-Series in Public Clouds)

Layer 3 segmentation ensures security policies are enforced at the right boundary to isolate traffic within Azure's virtual networks.

Question: 54

A primary firewall in a high availability (HA) pair is experiencing a current failover issue with ICMP pings to a secondary device. Which metric should be reviewed for proper ICMP pings between the firewall pair?

A. Link monitoring

B. Non-functional state

C. Heartbeat polling

D. Bidirectional Forwarding Detection (BFD)

Answer: C

Explanation:

Heartbeat polling is a core HA function to monitor connectivity between HA peers, leveraging ICMP pings to determine link health and availability.

"Heartbeat Polling uses ICMP pings to verify the connectivity and health of the HA peers. If heartbeat polling fails, the firewall considers the peer to be down and may initiate failover."

(Source: HA Link and Path Monitoring)

If ICMP pings fail, checking heartbeat polling logs helps identify if link or path monitoring triggers the failover.

Question: 55

What are two recommendations to ensure secure and efficient connectivity across multiple locations in a distributed enterprise network? (Choose two.)

A. Use Prisma Access to provide secure remote access for branch users.

B. Employ centralized management and consistent policy enforcement across all locations.

C. Create broad VPN policies for contractors working at branch locations.

D. Implement a flat network design for simplified network management and reduced overhead.

Answer: A, B

Explanation:

Prisma Access for secure remote access

"Prisma Access extends consistent security and optimized connectivity to branch locations, enabling secure access for mobile and branch users."

(Source: Prisma Access Overview)

Centralized management for consistent policy enforcement

"Centralized management using Strata Cloud Manager or Panorama ensures security policies and updates are uniformly applied across distributed locations, preventing policy drift and security gaps."

(Source: Strata Cloud Manager Best Practices)

These two practices are foundational for modern, distributed enterprise networks to maintain security posture and performance.

Question: 56

Which two configurations are required when creating deployment profiles to migrate a perpetual VM-Series firewall to a flexible VM? (Choose two.)

A. Choose "Fixed vCPU Models" for configuration type.

B. Allocate the same number of vCPUs as the perpetual VM.

C. Allow only the same security services as the perpetual VM.

D. Deploy virtual Panorama for management.

Answer: B, C

Explanation:

When migrating from a perpetual VM-Series firewall license to a flexible VM licensing model, two critical steps are needed:

Allocate same number of vCPUs – This ensures that the VM-Series capacity remains consistent and avoids resource bottlenecks.

"When migrating perpetual VM-Series licenses to flexible VM licensing, allocate the same vCPU and memory resources to ensure equivalent performance."

(Source: VM-Series Flexible Licensing Migration)

Limit to same security services – Flexible licensing requires maintaining the same security services to preserve licensing compliance.

"Ensure that you allow only the same security services on the flexible VM instance as were licensed on the perpetual VM."

(Source: Flexible Licensing and Service Subscriptions)

Question: 57

What occurs when a security profile group named "default" is created on an NGFW?

A. It only applies to traffic that has been dropped due to the reset client action.

B. It allows traffic to bypass all security checks by default.

C. It negates all existing security profiles rules on new policy.

D. It is automatically applied to all new security rules.

Answer: D

Explanation:

A security profile group named "default" is automatically applied to all new security rules unless a specific profile group is explicitly configured.

"If a security profile group named 'default' exists, it will be automatically applied to any newly created security policy rules to ensure consistent protection."

(Source: Security Profile Groups)

This behavior ensures that newly created policies are always protected by default security profiles, minimizing human error.

Question: 58

In a service provider environment, what key advantage does implementing virtual systems provide for managing multiple customer environments?

A. Shared threat prevention policies across all tenants

B. Centralized authentication for all customer domains

C. Unified logging across all virtual systems

D. Logical separation of control and Security policy

Answer: D

Explanation:

Virtual systems provide logical separation in a single physical firewall, allowing different customers (or tenants) to have isolated control and security policies.

"Virtual systems enable service providers to offer logically separated, independent environments on a single firewall. Each virtual system can have its own security policies, interfaces, and administrators."

(Source: Virtual Systems)

This ensures secure, tenant-specific segmentation within multi-tenant environments.

Question: 59

An administrator wants to implement additional Cloud-Delivered Security Services (CDSS) on a data center NGFW that already has one enabled. What benefit does the NGFW's single-pass parallel processing (SP3) architecture provide?

A. It allows for traffic inspection at the application level.

B. There will be no additional performance degradation.

C. There will be only a minor reduction in performance.

D. It allows additional security inspection devices to be added inline.

Answer: C

Explanation:

The SP3 architecture of Palo Alto NGFWs ensures that additional security services (CDSS) only cause a minor reduction in performance, as traffic is inspected once in a single pass.

"The single-pass parallel processing (SP3) architecture performs application identification and security enforcement simultaneously in one pass, resulting in only minor performance impacts when enabling multiple security services."

(Source: SP3 Architecture)

Unlike traditional multi-pass engines, SP3 architecture optimizes performance while delivering comprehensive security.

Question: 60

How can a firewall administrator block a list of 300 unique URLs in the most time-efficient manner?

A. Use application filters to block the App-IDs.

B. Use application groups to block the App-IDs.

C. Import the list into a custom URL category.

D. Block multiple predefined URL categories.

Answer: C

Explanation:

For large lists of specific URLs, creating a custom URL category and importing the list is the most efficient approach for granular URL filtering.

"You can create custom URL categories to define specific URLs or patterns and enforce policies for these categories. This is the most efficient way to handle large sets of URLs."

(Source: Custom URL Categories)

This approach saves time compared to manual rule creation or using generic application filters.