Vendor: Palo Alto Networks

Exam Code: NetSec-Pro

Exam Name: Palo Alto Networks Certified Network Security Professional

Version: DEMO

QUESTION 1
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.

QUESTION 2
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.

QUESTION 3
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.

QUESTION 4
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.

QUESTION 5
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.

QUESTION 6
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: CD
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.

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.

QUESTION 7
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: BC
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.

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.

QUESTION 8
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.

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

QUESTION 9
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.

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

QUESTION 10
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.

This data-driven approach avoids unnecessary configuration changes.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**