Vendor: Palo Alto Networks

Exam Code: PSE-Strata

Exam Name: Palo Alto Networks System Engineer - Strata

Version: DEMO

QUESTION 1
What is the key benefit of Palo Alto Networks Single Pass Parallel Processing design?

A. There are no benefits other than slight performance upgrades
B. It allows Palo Alto Networks to add new functions to existing hardware
C. Only one processor is needed to complete all the functions within the box
D. It allows Palo Alto Networks to add new devices to existing hardware

Answer: C

QUESTION 2
Which security profile on the NGFW includes signatures to protect you from brute force attacks?

A. Zone Protection Profile
B. URL Filtering Profile
C. Vulnerability Protection Profile
D. Anti-Spyware Profile

Answer: C

QUESTION 3
The need for a file proxy solution, virus and spyware scanner, a vulnerability scanner, and HTTP decoder for URL filtering is handled by which component in the NGFW?

A. First Packet Processor
B. Stream-based Signature Engine
C. SIA (Scan It All) Processing Engine
D. Security Processing Engine

Answer: B
Explanation:
https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdfn (page 6)

QUESTION 4
A customer is looking for an analytics tool that uses the logs on the firewall to detect actionable events on the network. They require something to automatically process a series of related threat events that, when combined, indicate a likely compromised host on their network or some other higher level conclusion. They need to pinpoint the area of risk, such as compromised hosts on the network, allows you to assess the risk and take action to prevent exploitation of network resources.

Which feature of PAN-OS can you talk about to address their requirement to optimize their business outcomes?

A. The Automated Correlation Engine
B. Cortex XDR and Cortex Data Lake
C. WildFire with API calls for automation
D. 3rd Party SIEM which can ingest NGFW logs and perform event correlation

Answer: A
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/use-the-automated-correlation-engine.html

QUESTION 5
Which two email links, contained in SMTP and POP3, can be submitted from WildFire analysis with a WildFire subscription? (Choose two.)

A. FTP
B. HTTPS
C. RTP
D. HTTP

Answer: BD

QUESTION 6
What two types of certificates are used to configure SSL Forward Proxy? (hoose two.)

A. Enterprise CA-signed certificates
B. Self-Signed certificates
C. Intermediate certificates
D. Private key certificates

Answer: AB

QUESTION 7
Which two of the following does decryption broker provide on a NGFW? (Choose two.)

A. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic only once
B. Eliminates the need for a third party SSL decryption option which allows you to reduce the total number of third party devices performing analysis and enforcement
C. Provides a third party SSL decryption option which allows you to increase the total number of third party devices performing analysis and enforcement
D. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic multiple times

Answer: AB
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker.html

QUESTION 8
There are different Master Keys on Panorama and managed firewalls.

What is the result if a Panorama Administrator pushes configuration to managed firewalls?

A. The push operation will fail regardless of an error or not within the configuration itself
B. Provided there's no error within the configuration to be pushed, the push will succeed

C. The Master Key from the managed firewalls will be overwritten with the Master Key from Panorama

D. There will be a popup to ask if the Master Key from the Panorama should replace the Master Key from the managed firewalls

Answer: A
Explanation:
https://www.reddit.com/r/paloaltonetworks/comments/onz15y/what_is_the_result_if_a_panorama_administrator/

QUESTION 9
Which task would be identified in Best Practice Assessment tool?

A. identify the visibility and presence of command-and-control sessions
B. identify sanctioned and unsanctioned SaaS applications
C. identify the threats associated with each application
D. identify and provide recommendations for device management access

Answer: B

QUESTION 10
A customer requests that a known spyware threat signature be triggered based on a rate of occurrence, for example, 10 hits in 5 seconds.

How is this goal accomplished?

A. Create a custom spyware signature matching the known signature with the time attribute
B. Add a correlation object that tracks the occurrences and triggers above the desired threshold
C. Submit a request to Palo Alto Networks to change the behavior at the next update
D. Configure the Anti-Spyware profile with the number of rule counts to match the occurrence frequency

Answer: A

QUESTION 11
Which two features are found in Palo Alto Networks NGFW but are absent in a legacy firewall product? (Choose two.)

A. Policy match is based on application
B. Traffic control is based on IP, port, and protocol
C. Traffic is separated by zones
D. Identification of application is possible on any port

Answer: AD

QUESTION 12
For customers with high bandwidth requirements for Service Connections, what two limitations exist when onboarding multiple Service Connections to the same Prisma Access location servicing a single Datacenter? (Choose two.)

A. Network segments in the Datacenter need to be advertised to only one Service Connection
B. The customer edge device needs to support policy-based routing with symmetric return functionality
C. The resources in the Datacenter will only be able to reach remote network resources that share the same region
D. A maximum of four service connections per Datacenter are supported with this topology

Answer: AD

QUESTION 13
Which three categories are identified as best practices in the Best Practice Assessment tool?
(Choose three.)

A. use of device management access and settings
B. identify sanctioned and unsanctioned SaaS applications
C. expose the visibility and presence of command-and-control sessions
D. measure the adoption of URL filters, App-ID, User-ID
E. use of decryption policies

Answer: BDE

QUESTION 14
You have a prospective customer that is looking for a way to provide secure temporary access to contractors for a designated period of time. They currently add contractors to existing user groups and create ad hoc policies to provide network access. They admit that once the contractor no longer needs access to the network, administrators are usually too busy to manually delete policies that provided access to the contractor. This has resulted in over-provisioned access that has allowed unauthorized access to their systems.

They are looking for a solution to automatically remove access for contractors once access is no longer required.

You address their concern by describing which feature in the NGFW?

A. Dynamic User Groups
B. Dynamic Address Groups
C. Multi-factor Authentication
D. External Dynamic Lists

Answer: A

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