

PSE-STRATA^{Q&As}

Palo Alto Networks System Engineer Professional-Strata

Pass PSE-STRATA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/pse-strata.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Official
Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

Which two configuration items are required when the NGFW needs to act as a decryption broker for multiple transparent bridge security chains? (Choose two.)

- A. dedicated pair of decryption forwarding interfaces required per security chain
- B. a unique Transparent Bridge Decryption Forwarding Profile to a single Decryption policy rule
- C. a unique Decryption policy rule is required per security chain
- D. a single pair of decryption forwarding interfaces

Correct Answer: BC

QUESTION 2

Which are the three mandatory components needed to run Cortex XDR? (Choose three.)

- A. Panorama
- B. NGFW with PANOS 8 0.5 or later
- C. Cortex Data Lake
- D. Traps
- E. Pathfinder
- F. Directory Syn Service

Correct Answer: BCF

<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture>

QUESTION 3

An Administrator needs a PDF summary report that contains information compiled from existing reports based on data for the Top five(5) in each category Which two timeframe options are available to send this report? (Choose two.)

- A. Daily
- B. Monthly
- C. Weekly
- D. Bi-weekly

Correct Answer: AC

QUESTION 4

Which Palo Alto Networks security component should an administrator use to and NGFW policies to remote users?

- A. Prisma SaaS API
- B. Threat intelligence Cloud
- C. GlobalProtect
- D. Cortex XDR

Correct Answer: C

QUESTION 5

Access to a business site is blocked by URL Filtering inline machine learning (ML) and considered as a false-positive.

How should the site be made available?

- A. Disable URL Filtering inline ML
- B. Create a custom URL category and add it to the Security policy
- C. Create a custom URL category and add it on exception of the inline ML profile
- D. Change the action of real-time detection category on URL filtering profile

Correct Answer: C

QUESTION 6

Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)

- A. Quarantine
- B. Allow
- C. Reset
- D. Redirect
- E. Drop
- F. Alert

Correct Answer: BCEF

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles.html>

QUESTION 7

A prospective customer currently uses a firewall that provides only Layer 4 inspection and protections. The customer sees traffic going to an external destination, port 53, but cannot determine what Layer 7 application traffic is going over that port

Which capability of PAN-OS would address the customer's lack of visibility?

- A. Device ID, because it will give visibility into which devices are communicating with external destinations over port 53
- B. single pass architecture (SPA), because it will improve the performance of the Palo Alto Networks Layer 7 inspection
- C. User-ID, because it will allow the customer to see which users are sending traffic to external destinations over port 53
- D. App-ID, because it will give visibility into what exact applications are being run over that port and allow the customer to block unsanctioned applications using port 53

Correct Answer: D

QUESTION 8

When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?

- A. X-Forwarded-For
- B. HTTP method
- C. HTTP response status code
- D. Content type

Correct Answer: A

QUESTION 9

Which of the following statements is valid with regard to Domain Name System (DNS) sinkholing?

- A. it requires the Vulnerability Protection profile to be enabled
- B. DNS sinkholing signatures are packaged and delivered through Vulnerability Protection updates
- C. infected hosts connecting to the Sinkhole Internet Protocol (IP) address can be identified in the traffic logs
- D. It requires a Sinkhole license in order to activate

Correct Answer: C

QUESTION 10

Which two features can be enabled to support asymmetric routing with redundancy on a Palo Alto networks next-generation firewall (NGFW)? (Choose two.)

- A. Active / active high availability (HA)
- B. Multiple virtual systems
- C. non-SYN first packet
- D. Asymmetric routing profile

Correct Answer: AC

QUESTION 11

Which two configuration elements can be used to prevent abuse of stolen credentials? (Choose two.)

- A. WildFire analysis
- B. Dynamic user groups (DUGs)
- C. Multi-factor authentication (MFA)
- D. URL Filtering Profiles

Correct Answer: CD

QUESTION 12

Which two methods are used to check for Corporate Credential Submissions? (Choose two.)

- A. domain credentialiter
- B. User-ID credential check
- C. LDAP query
- D. IP user mapping

Correct Answer: AB

QUESTION 13

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

Correct Answer: AD

QUESTION 14

Which four steps of the cyberattack lifecycle does the Palo Alto Networks Security Operating Platform prevent? (Choose four.)

- A. breach the perimeter
- B. weaponize vulnerabilities
- C. lateral movement
- D. exfiltrate data
- E. recon the target
- F. deliver the malware

Correct Answer: ACDF

QUESTION 15

Within the Five-Step Methodology of Zero Trust, in which step would application access and user access be defined?

- 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 1: Define the Protect Surface
- E. Step 2 Map the Protect Surface Transaction Flows

Correct Answer: D

[PSE-STRATA PDF Dumps](#) [PSE-STRATA VCE Dumps](#) [PSE-STRATA Practice Test](#)