



EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!



We offer free update service for one year!

<http://www.endexam.com>

Exam : **PCNSE**

Title : Paloalto Networks Palo Alto
Networks Certified Network
Security Engineer Exam

Version : DEMO

1.How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Answer: D

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewall-configurations

2.Which log file can be used to identify SSL decryption failures?

- A. Configuration
- B. Threats
- C. ACC
- D. Traffic

Answer: D

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC>

3.A customer wants to set up a site-to-site VPN using tunnel interfaces?

Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. Vpn-tunnel.1024
- B. vpn-tunne.1
- C. tunnel 1025
- D. tunnel. 1

Answer: C,D

4.If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

Answer: B

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

5.A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections.

Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Answer: A,C

Explanation:

Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box. Choices are limited to applications currently in the App-ID database. Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS. Use CasesThree primary uses cases for Application Override Policy are:

To identify "Unknown" App-IDs with a different or custom application signature
To re-identify an existing application signature

To bypass the Signature Match Engine (within the SP3 architecture) to improve processing times
A discussion of typical uses of application override and specific implementation examples is here:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>