SPOTO PCNSE Exam Free Demo

QUESTION 1
An engineer wants to forward all decrypted traffic on a PA-850 firewall to a forensic tool with a decrypt mirror interface.
Which statement is true regarding the configuration of the Decryption Port Mirroring feature?

A. The engineer must assign the related virtual-router to the decrypt mirror interface.
B. The PA-850 firewall does not support decrypt mirror interface, so the engineer needs to upgrade the firewall to PA-3200 series.
C. The engineer must assign an IP from the same subnet with the forensic tool to the decrypt mirror interface.
D. The engineer should install the Decryption Port Mirror license and reboot the firewall

Correct Answer: D

QUESTION 2
A client wants to detect the use of weak and manufacturer-default passwords for IoT devices.
Which option will help the customer?

A. Configure an Anti-Spyware profile with alert mode.
B. Configure an Antivirus profile with alert mode
C. Configure a vulnerability Protection profile with alert mode.
D. Configure a Data Filtering profile with alert mode

Correct Answer: D

QUESTION 3
What is a correct statement regarding administrative authentication using external services with a local authorization method?

A. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
B. Prior to PAN-OS 10.2, an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
C. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall
D. Stating with PAN-OS 10.2, an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.

Correct Answer: A

QUESTION 4
A client is concerned about web shell attacks against their servers. Which profile will protect the individual servers?

A. DoS Protection profile
B. Anti-Spyware profile
C. Antivirus profile
D. Zone Protection profile

Correct Answer: B

QUESTION 5
A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped by the firewall, the administrator decides to enable packet buffer protection to protect against similar attacks. The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate. What else should the administrator do to stop packet buffers from being overflowed?

A. Enable packet buffer protection for the affected zones.
B. Apply DOS profile to security rules allow traffic from outside.
C. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.
D. Add a Zone Protection profile to the affected zones.

Correct Answer: A

QUESTION 6

A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system logs. What is the likely cause?

A. Dead Peer Detection is not enabled.
B. The log quota for GTP and Tunnel needs to be adjusted.
C. The Tunnel Monitor is not configured.
D. Tunnel Inspection settings are misconfigured.

Correct Answer: B

QUESTION 7

A Firewall Engineer is migrating a legacy firewall to a Palo Alto Networks firewall in order to use features like App-ID and SSL decryption. Which order of steps is best to complete this migration?

A. Configure SSL decryption without migrating port-based security rules to App-ID rules.
B. First implement SSL decryption; then migrate port-based rules to App-ID rules.
C. First migrate SSH rules to App-ID; then implement SSL decryption.
D. First migrate port-based rules to App-ID rules; then implement SSL decryption.

Correct Answer: D

QUESTION 8

An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

A. They can have a different bandwidth.
B. They can have a different interface type from an aggregate interface group.
C. They can have a different interface type such as Layer 3 or Layer 2.

D. They can have different hardware media such as the ability to mix fiber optic and copper.

Correct Answer: D

QUESTION 9
A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility. There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.
What is the best option for the administrator to take?

A. Configure vwire interfaces for segment X on the firewall.
B. Configure a Layer 3 interface for segment X on the firewall.
C. Configure the TAP interface for segment X on the firewall.
D. Configure a new vsys for segment X on the firewall.

Correct Answer: A

QUESTION 10
An administrator wants to enable the firewall to forward Decrypted SSL traffic for Wildfire analysis. Where is this configured?

A. in the Wildfire Profile that is associated with the Security policy that the traffic matches
B. in the Decryption Profile that is associated with the decryption policy that the traffic matches
C. in the Decryption Profile that is associated with the Security policy that the traffic matches
D. in the Device Content-ID settings, by enabling Allow Forwarding of Decrypted Content

Correct Answer: D