



KaozhengPro

IT認證考試題庫 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **NetSec-Pro**

Title : Palo Alto Networks Certified
Network Security
Professional

Version : DEMO

1.Which procedure is most effective for maintaining continuity and security during a Prisma Access data plane software upgrade?

- A. Back up configurations, schedule upgrades during off-peak hours, and use a phased approach rather than attempting a network-wide rollout.
- B. Use Strata Cloud Manager (SCM) to perform dynamic upgrades automatically and simultaneously across all locations at once to ensure network-wide uniformity.
- C. Disable all security features during the upgrade to prevent conflicts and re-enable them after completion to ensure a smooth rollout process.
- D. Perform the upgrade during peak business hours, quickly address any user-reported issues, and ensure immediate troubleshooting post-rollout.

Answer: A

Explanation:

The best practice for Prisma Access data plane upgrades involves backing up configurations, scheduling upgrades during off-peak hours, and using a phased approach to minimize disruption and maintain continuity.

As per the Palo Alto Networks documentation:

“To minimize disruptions, it is recommended to perform Prisma Access upgrades during non-business hours and in a phased manner, starting with less critical sites to validate the process before moving to critical locations. Backup configurations and validate the system’s readiness to avoid data loss and maintain service continuity.”

(Source: Prisma Access Best Practices)

2.An NGFW administrator is updating PAN-OS on company data center firewalls managed by Panorama.

Prior to installing the update, what must the administrator verify to ensure the devices will continue to be supported by Panorama?

- A. Device telemetry is enabled.
- B. Panorama is configured as the primary device in the log collecting group for the data center firewalls.
- C. All devices are in the same template stack.
- D. Panorama is running the same or newer PAN-OS release as the one being installed.

Answer: D

Explanation:

The firewall must be running a PAN-OS version that is supported by Panorama. This means that Panorama must be running the same or a newer PAN-OS version as the one being installed on the firewalls to maintain compatibility.

“Before you upgrade the firewall, ensure that Panorama is running the same or a later PAN-OS version than the firewall. Panorama must always be at the same or a higher version to maintain compatibility.”

(Source: Panorama Admin Guide – Upgrade Process)

3.In which two applications can Prisma Access threat logs for mobile user traffic be reviewed? (Choose two.)

- A. Prisma Cloud dashboard
- B. Strata Cloud Manager (SCM)
- C. Strata Logging Service

D. Service connection firewall

Answer: B, C

Explanation:

Threat logs for Prisma Access mobile users can be reviewed in both Strata Cloud Manager (SCM) and Strata Logging Service. Prisma Cloud and service connection firewalls are not directly tied to mobile user traffic logs.

“Prisma Access logs are available in the Strata Cloud Manager and can also be sent to the Strata Logging Service for detailed analysis and threat visibility.”

(Source: Prisma Access Administration Guide)

4. Which two tools can be used to configure Cloud NGFWs for AWS? (Choose two.)

A. Cortex XSIAM

B. Prisma Cloud management console

C. Panorama

D. Cloud service provider's management console

Answer: C, D

Explanation:

Cloud NGFW for AWS can be configured using Panorama for centralized management, as well as the AWS management console for native integration and configuration.

“You can configure Cloud NGFW for AWS using Panorama for centralized security management, or directly through the AWS management console to deploy and manage security services for your AWS resources.”

(Source: Cloud NGFW for AWS Guide)

5. Using Prisma Access, which solution provides the most security coverage of network protocols for the mobile workforce?

A. Explicit proxy

B. Client-based VPN

C. Enterprise browser

D. Clientless VPN

Answer: B

Explanation:

Client-based VPN solutions like GlobalProtect provide full coverage for the mobile workforce by extending the enterprise security stack to remote endpoints. It establishes a secure tunnel, allowing consistent security policies across the enterprise perimeter and the mobile workforce.

“GlobalProtect is a client-based VPN that provides secure, consistent protection for mobile users by extending the security capabilities of Prisma Access to remote endpoints, covering all network protocols.”

(Source: GlobalProtect Admin Guide)