DUMPSARENA

Palo Alto Networks Network Security Professional

Palo Alto Networks NetSec-Pro

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which two components of a Security policy, when configured, allow third-party contractors access to internal applications outside business hours? (Choose two.)

A. App-ID

B. Service

C. User-ID

D. Schedule

ANSWER: C D

Explanation:

To allow third-party contractors access to internal applications only outside business hours, you would: - Use **User-ID** to target the policy to the specific contractor users/groups (identity-based policy enforcement rather than relying only on IP addresses). - Use a **Schedule** on the Security policy rule to ensure the rule is active only during the defined time window (outside business hours). References: - User-ID overview: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview - Schedule objects (used on Security policy rules): https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-policy/schedule-objects

QUESTION NO: 2

Which firewall attribute can an engineer use to simplify rule creation and automatically adapt to changes in server roles or security posture based on log events?

A. Address objects

B. Dynamic Address Groups

C. Dynamic User Groups

D. Predefined IP addresses

ANSWER: B

Explanation:

Correct Answer: Dynamic Address Groups

Dynamic Address Groups (DAGs) let you build Security policy rules that automatically update membership based on tags (for example, tags applied by log-triggered automation, the XML API, Cortex XSOAR, or VM/endpoint integrations). As tags change when a server's role or security posture changes, the DAG membership updates automatically—so policies adapt without manually editing address objects or rules.

Reference: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-dynamic-address-groups-in-policy

QUESTION NO: 3

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 supports configuration and management either centrally from Panorama (Cloud Services plugin) or natively from within AWS using the AWS Management Console (the cloud service provider's management console). Tools like Cortex XSIAM and the Prisma Cloud management console are not the primary configuration interfaces for Cloud NGFW for AWS. References: - https://docs.paloaltonetworks.com/cloud-ngfw/aws/cloud-ngfw-aws-admin/getting-started-with-cloud-ngfw-for-aws - https://docs.paloaltonetworks.com/cloud-ngfw/aws/cloud-ngfw-aws-admin/manage-cloud-ngfw-for-aws/monitor-cloud-ngfw-for-aws-in-aws-console

QUESTION NO: 4

Which two SSH Proxy decryption profile settings should be configured to enhance the company"™s security posture? (Choose two.)

A. Block sessions when certificate validation fails.

B. Allow sessions with legacy SSH protocol versions.

C. Block connections that use non-compliant SSH versions.

D. Allow sessions when decryption resources are unavailable.

ANSWER: A C

Explanation:

To harden SSH decryption, configure the SSH Proxy profile to deny insecure/legacy protocol negotiation and to fail closed when trust checks do not pass. - **Block sessions when certificate validation fails**: prevents continuing SSH proxying when host key/certificate validation cannot be verified, reducing risk of man-in-the-middle and untrusted endpoints. - **Block connections that use non-compliant SSH versions**: enforces modern, approved SSH protocol versions/crypto and blocks deprecated or weak versions. References: - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-concepts/ssh-proxy - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/configure-ssh-proxy-decryption

QUESTION NO: 5

Which GlobalProtect configuration is recommended for granular security enforcement of remote user device posture?

A. Configuring host information profile (HIP) checks for all mobile users

B. Configuring a rule that blocks the ability of users to disable GlobalProtect while accessing internal applications

C. Implementing multi-factor authentication (MFA) for all users attempting to access internal applications

D. Applying log at session end to all GlobalProtect Security policies

ANSWER: A

Explanation:

For granular security enforcement based on remote user device posture (for example, OS version, patch level, disk encryption, and anti-malware status), the recommended GlobalProtect configuration is to use Host Information Profile (HIP) checks and then reference HIP objects/profiles in Security policy rules. HIP enables posture-based access control decisions beyond user identity alone. References: - https://docs.paloaltonetworks.com/globalprotect/10-2/globalprotect-admin/host-information - https://docs.paloaltonetworks.com/globalprotect/10-2/globalprotect-admin/host-information/hip-objects - https://docs.paloaltonetworks.com/globalprotect/10-2/globalprotect-admin/host-information/hip-profiles

QUESTION NO: 6

After a firewall is associated with Strata Cloud Manager (SCM), which two additional actions are required to enable management of the firewall from SCM? (Choose two.)

A. Deploy a service connection for each branch site and connect with SCM.

B. Configure NTP and DNS servers for the firewall.

C. Configure a Security policy allowing “stratacloudmanager.paloaltonetworks.com” for all users.

D. Install a device certificate.

ANSWER: B D

Explanation:

To manage a firewall from Strata Cloud Manager (SCM) after it is associated, the firewall must be able to securely authenticate to Palo Alto Networks cloud services and reliably resolve/reach required cloud endpoints. - Configure NTP and DNS servers: Correct time (NTP) is required for certificate validation and secure sessions, and DNS is required to resolve SCM/cloud service FQDNs. - Install a device certificate: The firewall uses a device certificate to authenticate and establish trust for cloud management connectivity. References: - https://docs.paloaltonetworks.com/strata-cloud-manager - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/certificate-management - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-setup/services-device-setup/configure-ntp

QUESTION NO: 7

Which two prerequisites must be evaluated when decrypting internet-bound traffic? (Choose two.)

A. RADIUS profile

B. Incomplete certificate chains

C. Certificate pinning

D. SAML certificate

ANSWER: B C

Explanation:

When implementing SSL Forward Proxy (outbound) decryption, you must evaluate common conditions that can prevent successful decryption or break applications:

Incomplete certificate chains: If a server does not provide a complete chain (intermediate CA certificates missing) or the firewall cannot build/validate the chain, certificate validation can fail and decryption may not work as expected.
Certificate pinning: Some applications (for example, many financial/health apps) pin a specific server certificate or public key. Because SSL Forward Proxy re-signs certificates, pinned applications detect the change and may fail connectivity.

References: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-concepts and https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-exclusions

QUESTION NO: 8

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 most effective procedure is to (1) back up/validate configuration and readiness, (2) schedule the change during off-peak/nonbusiness hours, and (3) use a phased/canary rollout (start with less critical sites/remote networks and expand after validation). This reduces user impact, allows quick rollback/containment if issues arise, and preserves security controls throughout the maintenance window. References: - https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-overview - https://live.paloaltonetworks.com/t5/prisma-access-discussions/prisma-access-upgrade-best-practices/td-p/ (community discussion of phased/nonbusiness-hours upgrade practices)

QUESTION NO: 9

What is the recommended upgrade path from PAN-OS 9.1 to PAN-OS 11.2?

A. 9.1 â†’ 11.0 â†’ 11.2

B. 9.1 â†’ 10.0 â†’ 11.

C. 9.1 â†’ 11.

D. 9.1 â†’ 10.0 â†’ 11.2

ANSWER: D

Explanation:

Palo Alto Networks requires upgrading to each intermediate major (feature) release when moving across multiple major PAN-OS versions. Skipping major releases is not supported. Therefore, to upgrade from PAN-OS 9.1 to PAN-OS 11.2, you must first upgrade to PAN-OS 10.0 and then to PAN-OS 11.2.

Recommended path: **9.1 → 10.0 → 11.2**

Reference: https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-upgrade/upgrade-pan-os/upgrade-considerations

QUESTION NO: 10

Which set of practices should be implemented with Cloud Access Security Broker (CASB) to ensure robust data encryption and protect sensitive information in SaaS applications?

A. Do not enable encryption for data-at-rest to improve performance.

B. Use default encryption keys provided by the SaaS provider.

C. Perform annual encryption key rotations.

D. Enable encryption for data-at-rest and in transit, regularly update encryption keys, and use strong encryption algorithms.

ANSWER: D

Explanation:

The correct practice set is to protect SaaS data comprehensively by encrypting both **data at rest** and **data in transit**, using **strong/modern encryption algorithms**, and applying **regular key rotation** (often integrated with enterprise key management/KMS where possible). This combination reduces risk from interception, storage compromise, and key exposure over time.

Why others are incorrect:

A is incorrect because disabling encryption at rest weakens confidentiality and is not a recommended security posture.
B is incorrect because relying only on provider-default keys may not meet enterprise control/compliance requirements; best practice is to manage and rotate keys per policy (often customer-managed keys where supported).
C is not the best answer because annual-only rotations may be too infrequent depending on policy/risk; the question asks for a robust set of practices (encryption at rest + in transit + regular key updates + strong algorithms).

References:

https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final (NIST guidance on key management and rotation considerations)
https://cloud.google.com/kms/docs/key-rotation (Example of industry key-rotation best practices and rationale)