PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Network Security Professional

Palo Alto Networks NetSec-Pro

Version Demo

Total Demo Questions: 10

Total Premium Questions: 106

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Plan	26
Topic 2, Configure	45
Topic 3, Deploy and Configure	13
Topic 4, Operate	19
Topic 5, Troubleshoot	3
Total	106

QUESTION NO: 1

What occurs when a security profile group named â€œdefaultâ€ is created on an NGFW?

A. It only applies to traffic that has been dropped due to the reset client action.

B. It allows traffic to bypass all security checks by default.

C. It negates all existing security profiles rules on new policy.

D. It is automatically applied to all new security rules.

ANSWER: D

Explanation:

It is automatically applied to all new security rules. Palo Alto Networks NGFWs recognize a Security Profile Group specifically named **default** as the default group for newly created security policy rules. When an administrator creates a new rule, the firewall attaches that group automatically, so the rule receives the group's configured inspection profiles without requiring the administrator to select the group manually for each new rule. This behavior is intended to promote consistent security-policy hygiene and reduce the chance that a newly added allow rule is deployed without threat-prevention inspection. The profiles included in the default group determine the protections applied, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, WildFire Analysis, File Blocking, Data Filtering, and DNS Security, according to the organization's configuration and licensing. Administrators should therefore populate and maintain the default group with the profile set appropriate for their environment before relying on this automation. Existing policy rules are not retroactively changed merely because the group is created; the automatic association applies when new rules are created. Palo Alto Networks documents Security Profile Groups and the special behavior of a group named **default** in its Security Profile Groups documentation and recommends applying security profiles to policies as part of its security-policy best practices.

QUESTION NO: 2

What statuses may appear when devices are added to the controllerâ€™s Devices inventory list?

A. Unclaimed indicates that the device is available in the inventory, but has not been claimed.

B. Offline indicates that the device is not yet communicating with the Prisma SD-WAN controller.

C. Online-Restricted means that the device is communicating with the Prisma SD-WAN controller, but has not yet been claimed.

D. Decommissioned indicates that the device is permanently deleted from the controller.

ANSWER: A

Explanation:

Unclaimed indicates that the device is available in the inventory, but has not been claimed. This is the applicable device-inventory status description. In Prisma SD-WAN, a device can be present in the tenant's inventory based on its serial number and authorization information before it is assigned or claimed for use at a site. The *Unclaimed* state identifies precisely that onboarding stage: the appliance is available to the controller organization, but it has not yet been associated with a site and activated through the claiming workflow. This inventory visibility enables administrators to prepare hardware for deployment, verify that devices are available, and subsequently claim the intended appliance as part of site configuration. Palo Alto Networks documents Prisma SD-WAN device and site administration in the Prisma SD-WAN documentation portal, including inventory and onboarding workflows. For product documentation and release-specific administrative guidance, see the Prisma SD-WAN Administration documentation.

QUESTION NO: 3

How does a firewall behave when SSL Inbound Inspection is enabled?

A. It acts transparently between the client and the internal server.

B. It decrypts inbound and outbound SSH connections.

C. It decrypts traffic between the client and the external server.

D. It acts as a man-in-the-middle between the client and the internal server.

ANSWER: D

Explanation:

When SSL Inbound Inspection is enabled, the firewall acts as a man-in-the-middle between an external client and an internal server. This decryption mode is intended for sessions initiated from outside the organization to a protected internal server, such as a public-facing HTTPS web server. To perform inspection, the firewall must have access to the internal server's certificate and corresponding private key. It uses that key material to establish and decrypt the encrypted session, inspect the plaintext traffic against Security policy and security profiles, and then re-encrypt traffic as it is forwarded to the server or client.

This behavior enables the firewall to apply threat prevention, vulnerability protection, antivirus, and other inspection controls to traffic that would otherwise remain encrypted. The client continues to connect to the internal server's published identity, while the firewall intermediates the TLS communication for inspection purposes. Palo Alto Networks distinguishes this from SSL Forward Proxy, which is used for outbound connections from internal clients to external servers. See the Palo Alto Networks SSL Inbound Inspection documentation and the Decryption documentation overview for configuration and operational details.

QUESTION NO: 4

Which two types of logs must be forwarded to Strata Logging Service for IoT Security to function? (Choose two.)

A. WildFire

B. Enhanced application

C. Threat

D. URL Filtering

ANSWER: B C

Explanation:

IoT Security requires **Enhanced application** logs and **Threat** logs to be forwarded to Strata Logging Service. Enhanced application logging supplies the detailed application-visibility telemetry that IoT Security uses when discovering network-connected devices, building device profiles, and classifying devices based on their observed communications. This enhanced context is important because identification depends on more than basic network attributes; it incorporates application behavior observed by the Palo Alto Networks firewall.

Threat logs provide the security-event telemetry that IoT Security uses to associate detected threats with an identified device and to assess potentially risky behavior. Forwarding this information enables IoT Security to surface device-related threat activity and support security analysis using the firewall's prevention findings. Palo Alto Networks documents the firewall integration requirement to forward enhanced application and threat log data to the logging service used by IoT Security. Review the configuration guidance in the IoT Security log-forwarding documentation and the Strata Logging Service documentation.

QUESTION NO: 5

A primary firewall in a high availability (HA) pair is experiencing a current failover issue with ICMP pings to a secondary device. Which metric should be reviewed for proper ICMP pings between the firewall pair?

A. Link monitoring

B. Non-functional state

C. Heartbeat polling

D. Bidirectional Forwarding Detection (BFD)

ANSWER: C

Explanation:

Heartbeat polling is the appropriate metric to review because it is the HA peer-reachability mechanism that uses ICMP echo requests and replies between the two firewalls. Each firewall polls the peer through the configured HA control-link path and tracks whether replies are received within the configured interval and threshold. Reviewing this setting confirms that the HA pair has a valid path for the ICMP probes, that the polling interval and failure threshold are appropriate for the environment, and that intermittent packet loss is not causing an unnecessary peer-down condition or failover event.

In addition to checking the heartbeat-polling configuration, an administrator should validate the operational status of the HA control link and any configured backup control link, because the firewalls can use those paths to maintain HA communication. The HA dashboard and system logs can help correlate missed heartbeat polls with the reported failover behavior. Palo Alto Networks documents that HA link heartbeats use ICMP to verify connectivity between peers and describes the relevant polling behavior and configuration considerations in its HA Link Heartbeats documentation. Additional HA monitoring concepts are available in the HA Concepts documentation.

QUESTION NO: 6

Which two compliance standards are supported by SCM compliance reports?

A. PCI-DSS

B. NIST

C. CIS

D. GDPR

ANSWER: B C

Explanation:

NIST and CIS are supported by Strata Cloud Manager (SCM) compliance reporting to help security teams measure firewall configuration posture against recognized security guidance. NIST-based reporting maps the evaluated configuration posture to the applicable NIST framework or control guidance, providing a structured way to identify configuration gaps and support governance, risk, and audit activities. CIS reporting evaluates the deployment against Center for Internet Security benchmark recommendations, which are prescriptive hardening practices intended to reduce exposure from insecure or unnecessary configuration choices. These reports provide actionable findings that administrators can use to prioritize remediation and demonstrate alignment with organizational security baselines. In practice, the value of both standards is that they translate technical firewall configuration and operational settings into a framework-oriented assessment that security and compliance stakeholders can review. Palo Alto Networks documents SCM configuration-management and reporting capabilities in its Strata Cloud Manager documentation. Additional context on Palo Alto Networks configuration guidance and CIS benchmarking is available in the CIS Benchmark guide.

QUESTION NO: 7

Which feature of SaaS Security will allow a firewall administrator to identify unknown SaaS applications in an environment?

A. App-ID Cloud Engine

B. App-ID

C. SaaS Data Security

D. Cloud Identity Engine

ANSWER: A

Explanation:

App-ID Cloud Engine is the SaaS Security capability designed to provide visibility into SaaS applications that might not yet be identified by the firewall's standard, locally available application signatures. It uses cloud-delivered application intelligence to analyze traffic and identify previously unknown SaaS applications in the organization's environment. This gives firewall administrators a practical way to discover SaaS usage that may be unsanctioned or unmanaged, then use that visibility as the basis for appropriate security policy and SaaS governance decisions. Palo Alto Networks describes the App-ID Cloud Engine as extending next-generation firewall SaaS visibility by identifying SaaS applications through cloud intelligence, including applications that are newly observed. The feature is part of SaaS Security for Next-Generation Firewall and is intended to complement the firewall's existing App-ID capabilities with continuously updated cloud-based identification. See the SaaS Security for Next-Generation Firewall overview and the App-ID Cloud Engine documentation.

QUESTION NO: 8

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:

Strata Cloud Manager (SCM) and **Strata Logging Service** are the appropriate applications for reviewing Prisma Access threat logs generated by mobile-user traffic. Strata Cloud Manager is Palo Alto Networks' cloud-delivered management experience for Strata products and services, providing centralized operational visibility and access to log-monitoring workflows. Administrators can use its log viewer to search, filter, investigate, and correlate security events, including threat activity associated with Prisma Access traffic.

Strata Logging Service is the cloud logging platform that stores and makes available firewall and Prisma Access telemetry for analysis. It supports the retention, querying, and investigation of log types such as Threat logs, allowing security teams to identify detected threats, inspect event details, and use the data for incident response and reporting. Together, the management interface and cloud logging capability provide the expected workflow for operational review of mobile-user threat events in Prisma Access. Palo Alto Networks documents log viewing in View and Manage Logs and Prisma Access log collection and visibility in Logging for Prisma Access.

QUESTION NO: 9

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

A. Block sessions when SSH server certificate validation fails.

B. Allow sessions with legacy SSH protocol versions.

C. Block connections that use SSH protocol versions other than SSHv2.

D. Allow sessions when decryption resources are unavailable.

ANSWER: A C

Explanation:

SSH Proxy decryption should be configured to block sessions when SSH server certificate validation fails and to block connections that use SSH protocol versions other than SSHv2. Blocking a session after failed server-certificate validation ensures the firewall does not continue proxying a connection when it cannot establish trust in the server identity. This supports protection against connections to untrusted servers and possible man-in-the-middle activity, because the device fails closed rather than allowing an unverifiable SSH session to proceed.

Requiring SSHv2 is also an important baseline control. SSHv2 is the supported modern SSH protocol version and provides the security architecture required for robust SSH communications. Enforcing this version through the SSH Proxy decryption profile prevents SSH traffic that does not meet the organization's approved protocol standard from bypassing that baseline. Together, validation failure blocking and SSHv2 enforcement make decrypted SSH traffic subject to both endpoint-trust and protocol-compliance checks. Palo Alto Networks documents these SSH Proxy profile controls, including blocking sessions for SSH server certificate validation failures and for SSH versions other than version 2, in its SSH Proxy overview and SSH Proxy configuration guidance.

QUESTION NO: 10

Which two GlobalProtect modes allow partial users to access internal apps via GlobalProtect while other users access internal apps through third-party VPN?

A. Proxy

B. Hybrid, Proxy + Tunnel

C. Clientless VPN only

D. Always-On Tunnel only

ANSWER: A B

Explanation:

Proxy and **Hybrid, Proxy + Tunnel** are the GlobalProtect modes intended to support coexistence with another VPN client during a staged migration. In proxy mode, GlobalProtect can provide application access without requiring all endpoint traffic to be carried in a full GlobalProtect tunnel. This lets selected users begin using GlobalProtect for protected internal resources while users who have not yet migrated can continue to use an existing third-party VPN solution.

Hybrid mode combines proxy-based access with tunnel-based access. Administrators can use the proxy component for applications that are appropriate for proxy access and use the tunnel component when network-level connectivity is required. This flexibility supports phased deployment and different access requirements across user populations without requiring every user to transition to GlobalProtect at once. Palo Alto Networks documents GlobalProtect as a framework that provides secure remote access through the GlobalProtect app, portal, and gateway, with deployment choices tailored to application and network-access requirements. See the GlobalProtect Components documentation and the GlobalProtect Administrator's Guide overview.