PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Certified Network Security Consultant

Palo Alto Networks PCNSC

Version Demo

Total Demo Questions: 17

Total Premium Questions: 171

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Plan and Design a Network Security Solution	12
Topic 2, Install and Configure a Network Security Solution	115
Topic 3, Maintain and Troubleshoot a Network Security Solution	44
Total	171

QUESTION NO: 1

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

A. When Panorama is reverted to an earlier PAN-OS release, variables used in template stacks will be removed automatically.

B. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or stacks.

C. An administrator must use the Expedition tool to adapt the configuration to the pre-pan-OS 8.1 state.

D. Administrators need to manually update variable characters to those to used in pre-PAN-OS 8.1.

ANSWER: A

Explanation:

When Panorama is downgraded from PAN-OS 8.1 to an earlier release, variables used in template stacks are automatically removed. This is an important planning consideration because PAN-OS 8.1 introduced support for using variables in template stacks, while the earlier Panorama software cannot retain that configuration construct. Before performing the downgrade, the administrator should export and preserve the running configuration and document the variable names, values, and every template setting that references them. Doing so allows the affected configuration to be rebuilt or converted to explicit values as appropriate after the downgrade. The automatic removal can affect device-specific settings delivered through a template stack, so administrators should validate the resulting configuration and commit status before pushing configuration to managed firewalls. A tested backup and a maintenance plan are especially important because configuration loss caused by a downgrade is not restored merely by reinstalling the earlier image. Palo Alto Networks documents the template-stack variable capability in its Panorama 8.1 new-features documentation and provides the supported process and precautions in the Downgrade Panorama documentation.

QUESTION NO: 2

Which option would an administration choose to define the certificate and protect that Panorama and its managed devices uses for SSL/ITS services?

A. Set Up SSL/TLS under Policies > Service/URL Category > Service.

B. Configure an SSL/TLS Service Profile.

C. Configure a Decryption Profile and select SSL/TLS services.

D. Set up Security policy rule to allow SSL communication.

ANSWER: B

Explanation:

Configure an SSL/TLS Service Profile. An SSL/TLS Service Profile is the Panorama and PAN-OS configuration object used to associate a server certificate with the SSL/TLS protocol settings used by a management-facing service. The selected certificate supplies the identity presented by Panorama or a managed firewall during the TLS handshake, while the profile specifies the permitted TLS versions and related cryptographic settings. This lets an administrator centrally define the certificate and the protection requirements for applicable services, rather than merely allowing traffic or defining inspection behavior. On Panorama, the profile can be configured and then applied to supported services so that administrative and device communications use the intended certificate and secure TLS parameters. The certificate itself must first be available in the relevant certificate store, including its private key when Panorama or the firewall must act as the TLS server. Palo Alto Networks documents SSL/TLS Service Profiles as the location for selecting the certificate and configuring TLS settings for services. See the SSL/TLS Service Profile documentation and the Panorama certificate management documentation.

QUESTION NO: 3

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.

What will be the destination IP Address in that log entry?

A. The IP Address of sinkhole.paloaltonetworks.com

B. The IP Address of the command-and-control server

C. The IP Address specified in the sinkhole configuration

D. The IP Address of one of the external DNS servers identified in the anti-spyware database

ANSWER: C

Explanation:

The IP Address specified in the sinkhole configuration is the destination address recorded for the relevant post-resolution connection in the traffic log. When DNS Security or an Anti-Spyware profile detects a DNS request for a known malicious domain and its action is configured as sinkhole, the firewall forges the DNS response and substitutes the configured sinkhole IPv4 or IPv6 address for the domain's legitimate address. The infected endpoint then attempts to connect to that substituted address, rather than to the actual command-and-control infrastructure. This connection creates a traffic log whose destination is the configured sinkhole address. Administrators can therefore filter Traffic logs by the sinkhole IP address to identify internal hosts that attempted to contact malicious domains. The sinkhole address is configured in the Anti-Spyware profile's DNS Signatures settings; Palo Alto Networks provides default sinkhole addresses but also supports custom addresses where appropriate. See Palo Alto Networks documentation on identifying hosts that generate DNS sinkhole alerts and the knowledge-base procedure for verifying DNS sinkhole operation.

QUESTION NO: 4

What is exchanged through the HA2 link?

A. hello heartbeats

B. User-ID in information

C. session synchronization

D. HA state information

ANSWER: C

Explanation:

Session synchronization is exchanged through the HA2 link. In a Palo Alto Networks active/passive or active/active high-availability deployment, HA2 is the dedicated data link used to synchronize runtime state information between peers. Most importantly, it carries session state so that, if a failover occurs, the newly active firewall can continue processing existing traffic flows with minimal interruption rather than requiring endpoints to establish entirely new sessions. This synchronized state can include details such as NAT translations, application/session information, and other flow-processing state needed for session continuity. HA2 also supports synchronization of additional data-plane runtime information, depending on the feature configuration, such as IPsec security-association state and forwarding-table information. Because this traffic can be substantial in high-throughput environments, Palo Alto Networks recommends using a dedicated, reliable, and sufficiently sized HA2 connection. The HA design separates this data-plane synchronization function from the control-plane communications handled by the HA control link. For details, see the Palo Alto Networks documentation on HA links and backup links and high availability concepts.

QUESTION NO: 5

During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. Application changed from content inspection

B. session application identified

C. pattern based application identification

D. application override policy match

ANSWER: B D

Explanation:

During application identification, the firewall first determines whether an existing session already has an application classification. The *session application identified* check allows subsequent packets in an established session to use the application information already learned for that session, rather than beginning classification again. This preserves session consistency and supports efficient enforcement of Security policy rules based on App-ID.

An *application override policy match* is also evaluated as part of this processing. An Application Override rule explicitly assigns a configured application to matching traffic, based on attributes such as source, destination, service, and ports. When such a rule matches, the firewall uses that specified application for the session instead of performing normal App-ID classification for the traffic. This behavior is useful when an application cannot be accurately identified through standard signatures or when a known, controlled traffic flow requires an explicit application assignment.

These checks are key points in the PAN-OS packet-flow and App-ID handling sequence, ensuring that application-aware policy enforcement has a reliable application value associated with the session. See Palo Alto Networks documentation on packet flow sequence and App-ID.

QUESTION NO: 6

Which two methods can be used to verify firewall connectivity to Autofocus? (Choose two.)

A. Check the WebUI Dashboard Autofocus widget

B. Check for WildFire forwarding logs.

C. Verify AutoFocus is enabled below Device Management tab

D. Verify AutoFocus status using the CLI "test"command.

E. Check the license

ANSWER: A D

Explanation:

The *Check the WebUI Dashboard Autofocus widget* method is valid because the AutoFocus widget on the firewall web interface provides a direct visual indication of the firewall's AutoFocus connection status. When the firewall can communicate with the AutoFocus cloud service, the widget displays its connected state and associated AutoFocus information. This makes it a practical GUI-based validation after configuration or during operational troubleshooting.

The *Verify AutoFocus status using the CLI "test"command.* method is also valid. The PAN-OS operational command `test autofocus status` queries and reports the firewall's AutoFocus connectivity status, providing a direct command-line verification method. This is especially useful when GUI access is unavailable or when an administrator needs to validate service reachability from a CLI session. Both methods specifically validate communication with AutoFocus rather than merely confirming that a related feature is configured. Palo Alto Networks documents AutoFocus status verification for firewalls in its Verify AutoFocus Status guide and documents relevant operational commands in the PAN-OS CLI Command Hierarchy.

QUESTION NO: 7

The firewall identified a popular application as a unknown-tcp. Which options are available to identify the application? (Choose two.)

A. Create a Security policy to identify the customer application.

B. Create a customer object for the customer application server to identify the custom application.

C. Submit an App-ID request to Palo Alto Networks.

D. Create a custom application.

ANSWER: C D

Explanation:

Submit an App-ID request to Palo Alto Networks is appropriate when the traffic is for a popular, broadly used application that is not currently identified by the installed App-ID content. Palo Alto Networks accepts application requests from customers and can evaluate the traffic characteristics for inclusion in a future App-ID content release. Providing useful packet captures and details about the application helps Palo Alto Networks develop an accurate signature, which can then be distributed through dynamic updates and used consistently across firewalls.

Create a custom application is also available when the administrator needs to identify traffic locally, particularly when immediate control or visibility is needed. A custom App-ID can use protocol, port, IP protocol, and signature criteria to recognize the application's traffic. After defining the custom application, it can be used in Security policy rules, logging, reporting, and other policy controls just like predefined applications. This gives the organization a practical way to classify currently unknown traffic while an official App-ID is unavailable or when the application is proprietary or environment-specific. See Palo Alto Networks guidance for managing custom applications and the Customer Support Portal for submitting requests to Palo Alto Networks.

QUESTION NO: 8

Which version of Global Protect supports split tunneling based on destination domain, client process, and HTTP/HTTPs video streaming application?

A. Glovbalprotect version 4.0 with PAn-OS 8.0

B. Glovbalprotect version 4.1 with PAn-OS 8.1

C. Glovbalprotect version 4.0 with PAn-OS 8.1

D. Glovbalprotect version 4.1 with PAn-OS 8.0

E. GlobalProtect app version 5.0 with PAN-OS 8.1

ANSWER: E

Explanation:

GlobalProtect app version 5.0 with PAN-OS 8.1 introduced the expanded split-tunneling capabilities addressed in the question. This release combination allows an administrator to define traffic that bypasses the GlobalProtect tunnel using destination domains, endpoint processes or applications, and HTTP/HTTPS video-streaming traffic. These criteria supplement traditional route-based split tunneling and enable more targeted decisions about which traffic must traverse the corporate security infrastructure versus which traffic can use the user's local internet connection.

The GlobalProtect gateway configuration delivers the split-tunnel settings to supported GlobalProtect endpoints as part of the portal and gateway configuration. PAN-OS 8.1 supplies the gateway-side feature support, while GlobalProtect app 5.0 provides the endpoint support needed to evaluate process-based, domain-based, and video-streaming exclusions. This pairing is therefore required when deploying all three of the split-tunneling methods named in the question. Palo Alto Networks documents the available split-tunnel match criteria and configuration workflow in the GlobalProtect split-tunnel documentation. Additional release-specific context is available in the PAN-OS 8.1 GlobalProtect feature documentation.

QUESTION NO: 9 - (SIMULATION)

Match the App-ID adoption task with its order in the process.

ANSWER: See the explanation for the answer

Explanation:

Correct App-ID adoption order:

This sequence first preserves connectivity using the existing Layer 3/4 policy logic, then gathers traffic evidence. Application-based rules are introduced as clones of the legacy rules, validated by confirming traffic no longer matches the legacy rules, and only then are the old rules removed.

QUESTION NO: 10

An administrator has left a firewall to used default port for all management services. Which three function performed by the dataplane? (Choose three.)

A. NTP

B. antivirus

C. NAT

D. WildFire updates

E. file blocking

ANSWER: B C E

Explanation:

The dataplane is responsible for processing transit traffic as it passes through the firewall. This includes applying Security policy rules, performing address and port translation, and enforcing security services on matching sessions. Therefore, **NAT** is a dataplane function because translation is applied to packets and sessions that traverse the firewall. **antivirus** is also performed by the dataplane: after policy allows a session, the firewall's content-inspection engines examine applicable traffic for malware using configured Antivirus security profiles. Likewise, **file blocking** is enforced by the dataplane while inspecting allowed traffic; File Blocking profiles evaluate file transfers and take the configured action based on file type, direction, and application.

Leaving management services on their default ports does not alter this architecture. Management-plane services are used to administer the device and obtain operational resources, whereas the dataplane performs the real-time enforcement and inspection of user traffic. Palo Alto Networks describes the separation of management-plane and dataplane responsibilities in its PAN-OS architecture overview. Details on applying antivirus and file-blocking inspection through Security Profiles are available in the Security Profiles documentation.

QUESTION NO: 11

An administrator is configuring a Log Forwarding profile on a Palo Alto Networks NGFW.

Which three log types can be selected in a Log Forwarding profile match list? (Choose three.)

A. Traffic

B. Threat

C. URL

D. Configuration

E. System

ANSWER: A B C

Explanation:

Traffic, **Threat**, and **URL** are valid log types for Log Forwarding profile match lists. The administrator can define filters for each selected log type and configure actions such as forwarding logs to a syslog server, sending SNMP traps, generating email notifications, forwarding to Panorama, or registering tags.

Configuration and System logs are management-plane operational logs and are not selected as match-list log types in a Security policy Log Forwarding profile. Those logs can be viewed locally, forwarded through other logging mechanisms, or collected by Panorama, but they are not generated by a Security policy rule's Log Forwarding profile. Palo Alto Networks documents available Log Forwarding profile options in the Log Forwarding Profile documentation.

QUESTION NO: 12

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator Troubleshoot this issue? (Choose two.)

A. Perform a traffic pcap on the NGFW lo see any BGP problems

B. View the System logs and look for error messages about BGP

C. View the Runtime Stats and look for problems with BGP configuration

D. View the ACC lab to isolate routing issues.

ANSWER: B C

Explanation:

Viewing the System logs and looking for BGP-related error messages is useful because the firewall records relevant control-plane and routing-daemon events there. These events can reveal conditions that prevent BGP from learning or installing routes, such as peer establishment failures, configuration validation issues, or route-processing problems. Reviewing the log entries alongside the time at which the peer or routing change occurred provides important operational context.

Viewing Runtime Stats to inspect BGP configuration and operational status is also a primary troubleshooting method. The virtual router's runtime information shows the live BGP state rather than only the committed configuration. An administrator can verify peer status, session state, received and advertised prefixes, and the routes known to the routing process. This confirms whether the firewall is receiving updates and whether learned routes are eligible to enter the virtual router's forwarding table. The runtime view is therefore the appropriate place to distinguish a neighbor/session issue from a route-learning or route-installation issue.

Palo Alto Networks documents the Runtime Stats view for virtual-router and BGP operational information in the Virtual Router Runtime Stats documentation. For log investigation, consult the System Log Fields documentation.

QUESTION NO: 13

An organization has Palo Alto Networks MGfWs that sendlogs to remote monitoring and security management platforms. The network team has report has excessive traffic on the corporate WAN. How could the Palo Alto Networks NOFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

A. Forward logs from firewalls only to Panorama, and have Panorama forward logs to other external services.

B. Any configuration on an M-500 would address the insufficient bandwidth concerns.

C. Configure log compression and optimization features on all remote firewalls.

D. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.

ANSWER: A

Explanation:

Forward logs from firewalls only to Panorama, and have Panorama forward logs to other external services is correct because it centralizes log distribution at Panorama. Rather than each managed firewall sending duplicate copies of the same log records across the corporate WAN to several monitoring and security platforms, each firewall sends its logs once to Panorama. Panorama can then apply its Log Forwarding configuration to relay the appropriate received logs to the required external destinations, such as syslog servers, email recipients, SNMP managers, or HTTP-based services. This design substantially reduces repeated WAN transmissions from distributed firewall locations while preserving the existing downstream monitoring and security integrations. It also provides a central point at which administrators can manage filtering and forwarding behavior for logs generated by managed firewalls, making the logging architecture easier to operate consistently at scale. Palo Alto Networks documents the supported destination types and configuration workflow in Log Forwarding from Panorama to External Destinations. Centralized collection and management of firewall logs through Panorama is further described in the Centralized Firewall Logging documentation.

QUESTION NO: 14

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN -OS® software would help in this case?

A. content inspection

B. application override

C. Virtual Wire mode

D. redistribution of user mappings

ANSWER: D

Explanation:

Redistribution of user mappings is correct because it lets firewalls share learned IP-address-to-username mappings with other firewalls, reducing the need for every device to obtain the same mapping information directly from a centralized User-ID agent. In a large deployment, this distributes User-ID processing and communication closer to the enforcement points, which helps relieve traffic and processing pressure around the single User-ID agent server. A firewall can act as a redistribution point after learning mappings from sources such as an agent, server monitoring, or other supported User-ID mechanisms. Peer firewalls then receive the redistributed mappings and can use them for policy rules that reference users

and groups. This design is particularly useful where many firewalls require visibility into the same users but a centralized mapping source has become a scaling bottleneck. The redistribution configuration includes defining the mapping sources, selecting the redistribution agent or firewall role, and configuring the receiving firewalls to consume the redistributed information. Palo Alto Networks documents this capability in its Configure User Mapping Redistribution guidance and describes the broader architecture in the User-ID Deployment Options documentation.

QUESTION NO: 15

A Security policy rule is configured with a Vulnerability Protection Profile and an action of Deny".

Which action will this configuration cause on the matched traffic?

A. The configuration is invalid it will cause the firewall to Skip this Security policy rule A warning will be displayed during a command.

B. The configuration is valid It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny"

The configuration will allow the matched session unless a vulnerability signature is detected. The "Deny" action will supersede the per. defined, severity defined actions defined in the associated Vulnerability Protection Profile.

C. The configuration is invalid. The Profile Settings section will be grayed out when the action is set to "Deny"

ANSWER: C

Explanation:

The Profile Settings section is unavailable when a Security policy rule uses the *Deny* action. Vulnerability Protection is a Security Profile that performs inspection on traffic that a policy rule permits; it is not applied to traffic that is denied by the policy rule itself. In the PAN-OS web interface, selecting *Deny* prevents profile configuration for that rule by graying out the Profile Settings area. Therefore, a rule cannot be configured as described through the normal policy-rule configuration workflow: the firewall will not create a deny rule that evaluates matched traffic against the attached Vulnerability Protection Profile. This behavior ensures that Security Profiles are associated with rules that allow traffic to proceed far enough for App-ID, Content-ID, and threat inspection to occur. Palo Alto Networks documents the available Security policy rule actions and their behavior in its Security Policy Rule Actions documentation. For the relationship between Security policy rules and Security Profiles, see the Secure Traffic with Security Policy documentation.

QUESTION NO: 16

Which interface deployments support the Aggregate Ethernet Active configuration? (Choose three.)

A. LACP in TAP

B. LACP in Layer 3

C. LACP in Layer 2

D. LACP in Virtual Wire

E. LLDP in Layer 3

ANSWER: B C D

Explanation:

Aggregate Ethernet (AE) interfaces on Palo Alto Networks firewalls can be deployed as Layer 3, Layer 2, or Virtual Wire interfaces. In each of these deployments, configuring LACP in active mode enables the firewall to actively initiate Link Aggregation Control Protocol negotiation with its directly connected peer. The resulting AE bundle combines compatible physical Ethernet links into one logical interface, providing link redundancy and distributing traffic across member links according to the configured load-balancing behavior.

For **LACP in Layer 3**, the AE interface is a routed interface and can participate in IP routing and related Layer 3 services. For **LACP in Layer 2**, the AE interface operates as a switching interface and can be assigned to a VLAN. For **LACP in Virtual Wire**, the AE interface transparently forwards traffic between Virtual Wire zones while retaining the benefits of an aggregated, resilient link bundle. Palo Alto Networks documents these three interface types as supported AE deployments and documents active LACP as the mode in which the firewall sends LACP control packets to form the bundle.

See the Palo Alto Networks documentation on Aggregate Ethernet overview and LACP and LLDP support.

QUESTION NO: 17

Which two options prevents the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in milti-vsys mode.

B. The traffic does not match the packet capture filter

C. The traffic is offloaded.

D. The firewall's DP CPU is higher than 50%

ANSWER: B C

Explanation:

The traffic does not match the packet capture filter is correct because a Palo Alto Networks firewall records only packets that meet the configured packet-capture filters. Filters can constrain capture by attributes such as source or destination address, protocol, and port. Traffic that passes through the firewall but does not meet those criteria is deliberately excluded from the capture output. This lets an administrator isolate a relevant flow and avoid consuming capture-buffer capacity with unrelated packets.

The traffic is offloaded is also correct. A firewall can offload eligible sessions to hardware or fast-path processing to improve throughput. Because this traffic bypasses the normal software packet-processing path where dataplane packet capture is performed, it cannot be captured through the standard firewall packet-capture mechanism. When troubleshooting a flow, an administrator should therefore account for session offloading and, where appropriate, use the applicable troubleshooting workflow to ensure the needed traffic is processed in a manner visible to capture tools. Palo Alto Networks documents packet-capture setup, including filtering behavior, in its Take Packet Captures guidance. Additional platform and traffic-processing context is available in the Monitoring Overview.