

# Quiz Palo Alto Networks - NGFW-Engineer - Trustable Palo Alto Networks Next-Generation Firewall Engineer Study Test

## Your Guide to the Palo Alto Networks Next-Generation Firewall Engineer Certification: Skills, Scope, and Success



P.S. Free & New NGFW-Engineer dumps are available on Google Drive shared by ExamDiscuss: <https://drive.google.com/open?id=1KVCJsegZe1MqN4zLuzOE5XMlg4gLTkP>

To avoid this situation, we recommend you NGFW-Engineer real dumps. This product contains everything you need to crack the NGFW-Engineer certification exam on the first attempt. By choosing ExamDiscuss's updated dumps, you don't have to worry about appearing in the Palo Alto Networks Next-Generation Firewall Engineer (NGFW-Engineer) certification exam. ExamDiscuss Palo Alto Networks NGFW-Engineer Dumps are enough to get you through the Palo Alto Networks Next-Generation Firewall Engineer (NGFW-Engineer) actual exam on the first try.

### Palo Alto Networks NGFW-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>• PAN-OS Device Setting Configuration: This section evaluates the expertise of System Administrators in configuring device settings on PAN-OS. It includes implementing authentication roles and profiles, and configuring virtual systems with interfaces, zones, routers, and inter-VSYS security. Logging mechanisms such as Strata Logging Service and log forwarding are covered alongside software updates and certificate management for PKI integration and decryption. The section also focuses on configuring Cloud Identity Engine User-ID features and web proxy settings.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>• PAN-OS Networking Configuration: This section of the exam measures the skills of Network Engineers in configuring networking components within PAN-OS. It covers interface setup across Layer 2, Layer 3, virtual wire, tunnel interfaces, and aggregate Ethernet configurations. Additionally, it includes zone creation, high availability configurations (active and active</li> <li>• active and active</li> <li>• passive), routing protocols, and GlobalProtect setup for portals, gateways, authentication, and tunneling. The section also addresses IPsec, quantum-resistant cryptography, and GRE tunnels.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• Integration and Automation: This section measures the skills of Automation Engineers in deploying and managing Palo Alto Networks NGFWs across various environments. It includes the installation of PA-Series, VM-Series, CN-Series, and Cloud NGFWs. The use of APIs for automation, integration with third-party services like Kubernetes and Terraform, centralized management with Panorama templates and device groups, as well as building custom dashboards and reports in Application Command Center (ACC) are key topics.</li> </ul>

## Efficient NGFW-Engineer Study Test | Pass-Sure NGFW-Engineer Pass Guide and Trusted Palo Alto Networks Next-Generation Firewall Engineer Reliable Exam Pass4sure

ExamDiscuss NGFW-Engineer valid test will assist you to pass your NGFW-Engineer actual test with ease. You will never regret to choose our NGFW-Engineer exam engine test. Here are some outstanding properties which can benefit all of you. The detailed explanations are offered where available to ensure you fully understand why to choose the correct answers. All the questions cover the main points which the NGFW-Engineer Actual Exam required. The answers of each question are correct and verified by our IT experts which can ensure you 100% pass.

### Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q106-Q111):

#### NEW QUESTION # 106

After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish.

Which of the following actions will resolve this issue?

- A. Check that IPSec is enabled in the management profile on the external interface.
- B. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.
- C. Validate the tunnel interface VLAN against the peer's configuration.
- **D. Configure the Proxy IDs to match the Cisco ASA configuration.**

**Answer: D**

Explanation:

The Proxy IDs (or Traffic Selectors) define the local and remote subnets that are allowed to communicate over the IPSec tunnel. If the Proxy IDs on the Palo Alto Networks firewall do not match the configuration on the Cisco ASA, the tunnel will fail to establish because the firewalls won't agree on which traffic to encrypt.

Ensuring that the Proxy IDs match between the Palo Alto Networks firewall and the Cisco ASA will resolve the issue.

#### NEW QUESTION # 107

Which statement applies to Log Collector Groups?

- A. Log redundancy is available only if each Log Collector has the same amount of total disk storage.
- B. In any single Collector Group, all the Log Collectors must run on the same Panorama model.
- **C. The maximum number of Log Collectors in a Log Collector Group is 18 plus two hot spares.**
- D. Enabling redundancy increases the log processing traffic in a Collector Group by 50%.

**Answer: C**

Explanation:

The maximum number of Log Collectors that can be added to a Log Collector Group is 18 plus 2 hot spares, ensuring redundancy and availability in case of failure. This allows for a total of up to 20 Log Collectors in a group, providing sufficient scalability and reliability for log collection.

#### NEW QUESTION # 108

After a recent high availability (HA) failover test on an active/passive cluster, an engineer noted a 30-45 second delay before traffic started flowing through a Link Aggregation Control Protocol (LACP) aggregate interface on the newly active firewall.

What should have been configured to support LACP pre-negotiation to minimize LACP convergence delay?

- A. Set HA link monitoring to aggressive.
- B. Set LACP mode to passive.

- C. Enable LACP fast failover.
- **D. Enable in HA passive state.**

**Answer: D**

Explanation:

Enabling LACP in the HA passive state allows the passive firewall to negotiate and maintain the LACP session with the switch before it becomes active, so when a failover occurs the aggregate is already formed and traffic can pass with minimal convergence delay.

### NEW QUESTION # 109

A government agency needs to ensure that all user web access is explicitly mediated and authenticated. The agency has the following requirements:

- Client browsers must be manually configured to send traffic to the firewall's IP address and a specific port.
- The firewall must support seamless single sign-on (SSO) with the users' existing Active Directory credentials.

Which feature set should the engineer configure to meet the agency's requirements?

- A. Web proxy in transparent mode with an Authentication policy by using multi-factor authentication (MFA)
- **B. Web proxy in explicit mode with an Authentication policy by using Kerberos**
- C. User-ID agent integration with Authentication Portal for authentication
- D. Decryption policy that redirects users to a SAML identity provider for authentication

**Answer: B**

Explanation:

Explicit web proxy mode requires client browsers to be manually configured to send traffic to the firewall's IP address and port, and integrating it with an Authentication policy using Kerberos enables seamless single sign-on with Active Directory credentials through native domain authentication without additional user interaction.

### NEW QUESTION # 110

An NGFW engineer is configuring multiple Panorama-managed firewalls to start sending all logs to Strata Logging Service. The Strata Logging Service instance has been provisioned, the required device certificates have been installed, and Panorama and the firewalls have been successfully onboarded to Strata Logging Service.

Which configuration task must be performed to start sending the logs to Strata Logging Service and continue forwarding them to the Panorama log collectors as well?

- **A. Select the "Enable Cloud Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.**
- B. Modify all active Log Forwarding profiles to select the "Cloud Logging" option in each profile match list in the appropriate device groups.
- C. Enable the "Panorama/Cloud Logging" option in the Logging and Reporting Settings section under Device --> Setup --> Management in the appropriate templates.
- D. Select the "Enable Duplicate Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.

**Answer: A**

Explanation:

To begin sending logs to Strata Logging Service while continuing to forward them to Panorama log collectors, the necessary configuration is to enable Cloud Logging. This option is configured in the Cloud Logging section under Device # Setup # Management in the appropriate templates. Once enabled, this ensures that logs are directed both to the Strata Logging Service (cloud) and to the Panorama log collectors.

### NEW QUESTION # 111

.....

