



# **Paloalto-Networks**

## **Exam Questions NGFW-Engineer**

Palo Alto Networks Next-Generation Firewall Engineer

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

An enterprise uses GlobalProtect with both user- and machine-based certificate authentication and requires pre-logon, OCSP checks, and minimal user disruption. They manage multiple firewalls via Panorama and deploy domain-issued machine certificates via Group Policy. Which approach ensures continuous, secure connectivity and consistent policy enforcement?

- A. Use a wildcard certificate from a public CA, disable all revocation checks to reduce latency, and manage certificate renewals manually on each firewall.
- B. Distribute root and intermediate CAs via Panorama template, use distinct certificate profiles for user versus machine certs, reference an internal OCSP responder, and automate certificate deployment with Group Policy.
- C. Configure a single certificate profile for both user and machine certificate
- D. Rely solely on CRLs for revocation to minimize complexity.
- E. Deploy self-signed certificates on each firewall, allow IP-based authentication to override certificate checks, and use default GlobalProtect settings for user / machine identification.

**Answer: B**

#### Explanation:

To ensure continuous, secure connectivity and consistent policy enforcement with GlobalProtect in an enterprise environment that uses user- and machine-based certificate authentication, the approach should:

Distribute root and intermediate CAs via Panorama templates: This ensures that all firewalls managed by Panorama share the same trusted certificate authorities for consistency and security.

Use distinct certificate profiles for user vs. machine certificates: This enables separate handling of user and machine authentication, ensuring that both types of certificates are managed and validated appropriately.

Reference an internal OCSP responder: By integrating OCSP checks, the firewall can validate certificate revocation in real-time, meeting the security requirement while minimizing the overhead and latency associated with traditional CRLs (Certificate Revocation Lists).

Automate certificate deployment with Group Policy: This ensures that machine certificates are deployed in a consistent and scalable manner across the enterprise, reducing manual intervention and minimizing user disruption.

This approach supports the requirements for pre-logon, OCSP checks, and minimal user disruption, while maintaining a secure, automated, and consistent authentication process across all firewalls managed via Panorama.

### NEW QUESTION 2

Which statement applies to the relationship between Panorama-pushed Security policy and local firewall Security policy?

- A. When a policy match is found in a local firewall policy, if any Panorama shared post-rule is configured, it will still be evaluated.
- B. Local firewall rules are evaluated after Panorama pre-rules and before Panorama post- rules.
- C. Panorama post-rules can be configured to be evaluated before local firewall policy for the purpose of troubleshooting.
- D. The order of policy evaluation can be configured differently in different device groups.

**Answer: B**

#### Explanation:

Local firewall rules are evaluated after Panorama pre-rules (those applied before the firewall's local policies) and before Panorama post-rules (those applied after the firewall's local policies). This ensures that the local firewall rules do not override the central Panorama policy and are only applied in the appropriate order within the policy evaluation sequence.

### NEW QUESTION 3

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

**Answer: B**

#### 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 4

When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

- A. Service graph
- B. Ansible automation modules
- C. Panorama role-based access control
- D. CN-Series firewalls

**Answer: D**

#### Explanation:

When integrating Kubernetes with Palo Alto Networks NGFWs, the CN-Series firewalls are specifically designed to secure traffic between microservices in containerized environments. These firewalls provide advanced security features like Application Identification (App-ID), URL filtering, and Threat Prevention to secure communication between containers and microservices within a Kubernetes environment.

### NEW QUESTION 5

An engineer is implementing a new rollout of SAML for administrator authentication across a company's Palo Alto Networks NGFWs. User authentication on company firewalls is currently performed with RADIUS, which will remain available for six months, until it is decommissioned. The company wants both authentication types to be running in parallel during the transition to SAML.

Which two actions meet the criteria? (Choose two.)

- A. Create a testing and rollback plan for the transition from Radius to SAML, as the two authentication profiles cannot be run in tandem.
- B. Create an authentication sequence that includes both the RADIUS Server Profile and SAML Identity Provider Server Profile to run the two services in tandem.
- C. Create and apply an authentication profile with the SAML Identity Provider Server Profile.
- D. Create and add the SAML Identity Provider Server Profile to the authentication profile for the RADIUS Server Profile.

**Answer:** BD

**Explanation:**

To enable both RADIUS and SAML authentication to run in parallel during the transition period, you need to configure an authentication sequence and an authentication profile that includes both authentication methods.

By creating an authentication sequence that includes both RADIUS and SAML server profiles, the firewall will attempt authentication with RADIUS first and, if that fails, will fall back to SAML. This enables both authentication types to function simultaneously during the transition period.

You can also configure an authentication profile that includes both the RADIUS Server Profile and the SAML Identity Provider server profile. This setup allows the firewall to use both RADIUS and SAML for authentication requests, and it will check both authentication methods in parallel.

**NEW QUESTION 6**

Without performing a context switch, which set of operations can be performed that will affect the operation of a connected firewall on the Panorama GUI?

- A. Restarting the local firewall, running a packet capture, accessing the firewall CLI
- B. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostname
- C. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network Profile
- D. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reports

**Answer:** B

**Explanation:**

In Panorama, without performing a context switch, the administrator can perform local configuration tasks directly on the connected firewall. The following operations can be done:

Modification of local security rules: Security rules can be modified directly on the connected firewall from the Panorama GUI.

Modification of a Layer 3 interface: Changes to the Layer 3 interfaces on the connected firewall can be done from Panorama, without needing to switch to the firewall's local interface.

Modification of the firewall device hostname: The firewall's hostname can be changed via Panorama.

**NEW QUESTION 7**

Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?

- A. DDNS
- B. Link Duplex
- C. NetFlow
- D. LLDP

**Answer:** C

**Explanation:**

NetFlow is a Layer 3 (network layer) protocol that collects and monitors IP traffic flows. It is typically configured on Layer 3 interfaces because it relies on IP information for traffic flow analysis, which is not available on Layer 2 interfaces. Layer 2 interfaces handle frames within the local network, and they don't have IP-related details that NetFlow uses to generate traffic statistics.

**NEW QUESTION 8**

In an active/active high availability (HA) configuration with two PA-Series firewalls, how do the firewalls use the HA3 interface?

- A. To forward packets to the HA peer during session setup and asymmetric traffic flow
- B. To exchange hellos, heartbeats, HA state information, and management plane synchronization for routing and User-ID information
- C. To synchronize sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in an HA pair
- D. To perform session cache synchronization among all HA peers having the same cluster ID

**Answer:** D

**Explanation:**

In an active/active HA configuration with two PA-Series firewalls, the HA3 interface is used primarily for the exchange of HA state information between the firewalls. This includes: Hellos and heartbeats to monitor the status of the HA peer.

Synchronization of management plane data, which includes critical routing and User-ID information.

**NEW QUESTION 9**

Which configuration in the LACP tab will enable pre-negotiation for an Aggregate Ethernet (AE) interface on a Palo Alto Networks high availability (HA) active/passive pair?

- A. Set Transmission Rate to fast.
- B. Set passive link state to Auto.
- C. Set Enable in HA Passive State.
- D. Set LACP mode to Active.

**Answer:** C

**Explanation:**

In a High Availability (HA) active/passive pair configuration, when setting up an Aggregate Ethernet (AE) interface, enabling the "Enable in HA Passive State" option allows the interface to participate in LACP (Link Aggregation Control Protocol) even when the system is in the passive state. This ensures that the pre-negotiation of the LACP link occurs, allowing the link aggregation to be ready as soon as the firewall becomes active.

**NEW QUESTION 10**

Which two statements apply to configuring required security rules when setting up an IPSec tunnel between a Palo Alto Networks firewall and a third-party gateway? (Choose two.)

- A. For incoming and outgoing traffic through the tunnel, creating separate rules for each direction is optional.
- B. The IKE negotiation and IPSec/ESP packets are allowed by default via the intrazone default allow policy.
- C. For incoming and outgoing traffic through the tunnel, separate rules must be created for each direction.
- D. The IKE negotiation and IPSec/ESP packets are denied by default via the interzone default deny policy.

**Answer:** CD

**Explanation:**

Separate rules must be created for each direction: Palo Alto Networks firewalls enforce security policies based on traffic direction. To allow bidirectional communication through the IPSec tunnel, two separate rules are required - one for incoming and one for outgoing traffic.

IKE negotiation and IPSec/ESP packets are denied by default: Palo Alto Networks firewalls use an interzone default deny policy, meaning that unless an explicit policy allows IKE (UDP 500/4500) and ESP (protocol 50) traffic, the firewall will block these packets, preventing tunnel establishment. Therefore, administrators must create explicit rules permitting IKE and IPSec/ESP traffic to the firewall's external interface.

**NEW QUESTION 10**

An administrator plans to upgrade a pair of active/passive firewalls to a new PAN-OS release. The environment is highly sensitive, and downtime must be minimized.

What is the recommended upgrade process for minimal disruption in this high availability (HA) scenario?

- A. Suspend the active firewall to trigger a failover to the passive firewall
- B. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operation
- C. Then fail traffic back and upgrade the remaining firewall.
- D. Shut down the currently active firewall and upgrade it offline, allowing the passive firewall to handle all traffic
- E. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluster
- F. Finally, upgrade the passive firewall while the newly upgraded unit remains active.
- G. Isolate both firewalls from the production environment and upgrade them in a separate, offline setup
- H. Reconnect them only after validating the new software version, resuming HA functionality once both units are fully upgraded and tested.
- I. Push the new PAN-OS version simultaneously to both firewalls, having them upgrade and reboot in parallel
- J. Rely on automated HA reconvergence to restore normal operations without manually failing over traffic.

**Answer:** A

**Explanation:**

In an active/passive HA setup, the recommended process for upgrading involves minimizing downtime and ensuring traffic continuity by using the failover process: Suspend the active firewall: This triggers a failover to the passive unit, making it the active unit.

Upgrade the former passive (now active) unit: With traffic now running on the previously passive unit, upgrade the suspended unit while the active unit continues handling traffic. Confirm proper operation: Once the upgrade is complete, verify that the upgraded unit is functioning properly.

Fail traffic back: Once the upgraded firewall is confirmed to be working, fail the traffic back to the original active unit and upgrade the remaining firewall.

**NEW QUESTION 14**

.....

## Relate Links

**100% Pass Your NGFW-Engineer Exam with ExamBible Prep Materials**

<https://www.exambible.com/NGFW-Engineer-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>