



# **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

An organization runs multiple Kubernetes clusters both on-premises and in public clouds (AWS, Azure, GCP). They want to deploy the Palo Alto Networks CN-Series NGFW to secure east-west traffic within each cluster, maintain consistent Security policies across all environments, and dynamically scale as containerized workloads spin up or down. They also plan to use a centralized Panorama instance for policy management and visibility. Which approach meets these requirements?

- A. Install standalone CN-Series instances in each cluster with local configuration onl
- B. Export daily policy configuration snapshots to Panorama for recordkeeping, but do not unify policy enforcement.
- C. Configure the CN-Series only in public cloud clusters, and rely on Kubernetes Network Policies for on-premises cluster securit
- D. Synchronize partial policy information into Panorama manually as needed.
- E. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in eachcluster, ensuring local insertion into the service mesh or CN
- F. Manage all CN-Series firewalls centrally from Panorama, applying uniform Security policies across on-premises and cloud clusters.
- G. Deploy a single CN-Series firewall in the on-premises data center to process traffic for all clusters, connecting remote clusters via VPN or peerin
- H. Manage this single instance through Panorama.

**Answer: C**

#### Explanation:

This approach meets all the requirements for securing east-west traffic within each Kubernetes cluster, maintaining consistent security policies across on-premises and cloud environments, and allowing for dynamic scaling of the CN-Series NGFWs as containerized workloads spin up or down. By using Kubernetes-native deployment tools (such as Helm), the CN-Series NGFWs can be deployed and scaled dynamically within each cluster. Local insertion into the service mesh or CNI ensures that the NGFW can inspect traffic at the appropriate points within the cluster.

Centralized management via Panorama ensures that security policies are uniform across both on-premises and cloud environments, providing visibility and control across all clusters.

#### NEW QUESTION 3

What is the purpose of assigning an Admin Role Profile to a user in a Palo Alto Networks NGFW?

- A. Allow access to all resources without restrictions.
- B. Enable multi-factor authentication (MFA) for administrator access.
- C. Define granular permissions for management tasks.
- D. Restrict access to sensitive report data.

**Answer: C**

#### Explanation:

Assigning an Admin Role Profile to a user in a Palo Alto Networks NGFW is used to define granular permissions for management tasks. This allows administrators to control what actions a user can perform on the firewall, such as configuration changes, monitoring, and logging. By assigning different admin roles, you can ensure that users have access only to the areas and tasks they need, enforcing the principle of least privilege.

#### NEW QUESTION 4

Which statement describes the role of Terraform in deploying Palo Alto Networks NGFWs?

- A. It acts as a logging service for NGFW performance metrics.
- B. It orchestrates real-time traffic inspection for network segments.
- C. It provides Infrastructure-as-Code (IaC) to automate NGFW deployment.
- D. It manages threat intelligence data synchronization with NGFWs.

**Answer: C**

**Explanation:**

Terraform is an Infrastructure-as-Code (IaC) tool that automates the provisioning and management of infrastructure resources, including Palo Alto Networks Next-Generation Firewalls (NGFWs). By using Terraform configuration files, administrators can define and deploy NGFW instances across cloud environments (such as AWS, Azure, and GCP) efficiently and consistently.

Terraform enables:

Automated firewall deployment in cloud environments.

Configuration of security policies and networking settings in a declarative manner. Scalability and repeatability, reducing manual intervention in firewall provisioning.

**NEW QUESTION 5**

According to dynamic updates best practices, what is the recommended threshold value for content updates in a mission- critical network?

- A. 8 hours
- B. 16 hours
- C. 32 hours
- D. 48 hours

**Answer:** A

**Explanation:**

For a mission-critical network, it is recommended to configure the content update threshold to 8 hours. This ensures that the network is protected with the latest threat intelligence, updates to signatures, and other critical content, minimizing the exposure to newly discovered vulnerabilities and threats.

Regular content updates are crucial in mission-critical environments to ensure the firewall is up-to-date with the latest protections. 8 hours is considered an optimal balance between timely updates and network performance.

**NEW QUESTION 6**

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. Enabling redundancy increases the log processing traffic in a Collector Group by 50%.
- C. In any single Collector Group, all the Log Collectors must run on the same Panorama model.
- D. The maximum number of Log Collectors in a Log Collector Group is 18 plus two hot spares.

**Answer:** D

**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 7**

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 8**

Which type of firewall resource can be assigned when configuring a new firewall virtual system (VSYS)?

- A. ICPU
- B. Sessions limit
- C. Memory
- D. Security profile limit

**Answer:** B

**Explanation:**

When configuring a new firewall virtual system (VSYS) on a Palo Alto Networks firewall, one of the resources that can be assigned is the sessions limit. This setting allows the administrator to control the number of active sessions that can be handled by the VSYS, ensuring that each virtual system has an appropriate allocation of resources based on its needs.

**NEW QUESTION 9**

In regard to the Advanced Routing Engine (ARE), what must be enabled first when configuring a logical router on a PAN-OS firewall?

- A. License
- B. Plugin
- C. Content update
- D. General setting

**Answer:** A

**Explanation:**

To enable the Advanced Routing Engine (ARE) on a Palo Alto Networks firewall, the license for the ARE must be applied first. Without the proper license, the firewall cannot activate and use the advanced routing features provided by ARE, such as support for more complex routing protocols (e.g., BGP, OSPF, etc.). Once the license is applied and validated, the routing engine can be configured, allowing the creation of logical routers and routing policies.

**NEW QUESTION 10**

When deploying Palo Alto Networks NGFWs in a cloud service provider (CSP) environment, which method ensures high availability (HA) across multiple availability zones?

- A. Deploying Ansible scripts for zone-specific scaling
- B. Implementing Terraform templates for redundancy within one availability zone
- C. Using load balancer and health probes
- D. Configuring active/active HA

**Answer:** C

**Explanation:**

To ensure high availability (HA) across multiple availability zones (AZs) in a cloud service provider (CSP) environment, using a load balancer with health probes is a recommended method. This setup ensures that traffic can be directed to the healthy NGFW instances across multiple availability zones. If one NGFW instance or availability zone goes down, the load balancer can redirect traffic to the available instance(s) in other zones, providing redundancy and maintaining service availability.

**NEW QUESTION 10**

For which two purposes is an IP address configured on a tunnel interface? (Choose two.)

- A. Use of dynamic routing protocols
- B. Tunnel monitoring
- C. Use of peer IP
- D. Redistribution of User-ID

**Answer:** AB

**Explanation:**

Use of dynamic routing protocols: An IP address is needed on the tunnel interface to participate in dynamic routing protocols (like OSPF, BGP, etc.) over the tunnel. This allows the firewall to advertise routes and receive updates over the tunnel.

Tunnel monitoring: The IP address on the tunnel interface can also be used for monitoring the tunnel's status. Tunnel monitoring (such as IPSec tunnel monitoring) requires an IP address on the tunnel interface to check the health and availability of the tunnel.

**NEW QUESTION 13**

Which two zone types are valid when configuring a new security zone? (Choose two.)

- A. Tunnel
- B. Intrazone
- C. Internal
- D. Virtual Wire

**Answer:** AD

**Explanation:**

When configuring a new security zone on a Palo Alto Networks firewall, the two valid zone types are:

Tunnel: A Tunnel zone is used for traffic that is associated with a VPN tunnel, such as IPSec tunnels. Traffic passing through a tunnel interface is classified into this zone.

Virtual Wire: A Virtual Wire zone is used when a firewall operates in transparent mode (also known as Layer 2 mode). In this configuration, the firewall can inspect traffic without modifying the IP address structure of the network.

**NEW QUESTION 16**

Palo Alto Networks NGFWs use SSL/TLS profiles to secure which two types of connections? (Choose two.)

- A. NAT tables
- B. User Authentication
- C. GlobalProtect Gateways
- D. GlobalProtect Portal

**Answer:** CD

**Explanation:**

Palo Alto Networks Next-Generation Firewalls (NGFWs) use SSL/TLS profiles to secure connections for services such as GlobalProtect Gateways and GlobalProtect Portals. These profiles are used to manage the SSL/TLS encryption and decryption for secure communication between the firewall and clients (such as VPN clients for GlobalProtect). This helps ensure the confidentiality and integrity of the data during transmission.

**NEW QUESTION 19**

An NGFW engineer is configuring multiple Layer 2 interfaces on a Palo Alto Networks firewall, and all interfaces must be assigned to the same VLAN. During initial testing, it is reported that clients located behind the various interfaces cannot communicate with each other.

Which action taken by the engineer will resolve this issue?

- A. Configure each interface to belong to the same Layer 2 zone and enable IP routing between them.
- B. Assign each interface to the appropriate Layer 2 zone and configure a policy that allows traffic within the VLAN.
- C. Assign each interface to the appropriate Layer 2 zone and configure Security policies for interfaces not assigned to the same zone.
- D. Enable IP routing between the interfaces and configure a Security policy to allow traffic between interfaces within the VLAN.

**Answer:** B

**Explanation:**

In a Layer 2 configuration, interfaces are typically grouped into the same Layer 2 zone. When the interfaces are assigned to the same VLAN, the firewall will treat them as part of the same broadcast domain.

In a Layer 2 setup, interfaces must be in the same Layer 2 zone to allow the traffic within the same VLAN to pass. Additionally, a security policy must be configured to allow traffic within this VLAN or zone. This will resolve the issue by ensuring that traffic is permitted between clients behind different interfaces assigned to the same VLAN.

**NEW QUESTION 23**

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 26**

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 29**

In a hybrid cloud deployment, what is the primary function of Ansible in managing Palo Alto Networks NGFWs?

- A. It provides a web interface for managing NGFW hardware clusters.
- B. It enables centralized log collection and correlation for NGFWs.
- C. It facilitates dynamic updates to NGFW threat databases.
- D. It automates NGFW policy updates and configurations through playbooks.

**Answer:** D

**Explanation:**

In a hybrid cloud deployment, Ansible is primarily used for automating configurations and policy updates on Palo Alto Networks Next-Generation Firewalls (NGFWs). Through the use of playbooks, Ansible can automate the process of deploying security policies, updating configurations, and managing the firewall's state, which enhances efficiency and consistency across multiple NGFWs in a large or hybrid cloud environment.

**NEW QUESTION 34**

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 35

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 38

Which CLI command is used to configure the management interface as a DHCP client?

- A. set network dhcp interface management
- B. set network dhcp type management-interface
- C. set deviceconfig system type dhcp-client
- D. set deviceconfig management type dhcp-client

**Answer:** D

#### Explanation:

To configure the management interface as a DHCP client on a Palo Alto Networks NGFW, the correct CLI command is set deviceconfig management type dhcp-client.

This command configures the management interface to obtain an IP address dynamically using DHCP.

#### NEW QUESTION 41

Which two actions in the IKE Gateways will allow implementation of post-quantum cryptography when building VPNs between multiple Palo Alto Networks NGFWs? (Choose two.)

- A. Select IKE v2, enable the Advanced Options • PQ PPK, then set a 64+ character string for the post-quantum pre shared key.
- B. Ensure Authentication is set to ??certificate,?? then import a post-quantum derived certificate.
- C. Select IKE v2 Preferred, enable the Advanced Options • PQ KEM, then add one or more ??Rounds.??
- D. Select IKE v2, enable the Advanced Options • PQ KEM, then create an IKE Crypto Profile with Advanced Options adding one or more ??Rounds.??

**Answer:** CD

#### Explanation:

To implement post-quantum cryptography (PQC) in VPNs between Palo Alto Networks NGFWs, you would enable the PQ KEM (Post-Quantum Key Encapsulation Mechanism) in the IKE gateway configuration. This enables the firewall to use quantum-resistant encryption for key exchange, which is an essential part of securing communications against the potential future threats posed by quantum computing.

By selecting IKE v2 Preferred and enabling the PQ KEM option under Advanced Options, you can add specific Rounds for the post-quantum cryptography process, which will help in implementing quantum-resistant key exchange methods.

This option similarly selects IKE v2 and enables PQ KEM while also creating a dedicated IKE Crypto Profile with the necessary Rounds configured for post-quantum cryptography.

#### NEW QUESTION 44

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 48

An NGFW engineer is establishing bidirectional connectivity between the accounting virtual system (VSYS) and the marketing VSYS. The traffic needs to transition between zones without leaving the firewall (no external physical connections). The interfaces for each VSYS are assigned to separate virtual routers (VRs), and inter-VR static routes have been configured. An external zone has been created correctly for each VSYS. Security policies have been added to permit the desired traffic between each zone and its respective external zone. However, the desired traffic is still unable to successfully pass from one VSYS to the other in either direction.

Which additional configuration task is required to resolve this issue?

- A. Create a transit VSYS and route all inter-VSYS traffic through it.
- B. Add each VSYS to the list of visible virtual systems of the other VSYS.
- C. Enable the ??allow inter-VSYS traffic?? option in both external zone configurations.
- D. Create Security policies to allow the traffic between the two external zones.

**Answer:** B

#### Explanation:

In Palo Alto Networks firewalls, each virtual system (VSYS) is typically isolated from other VSYSs, meaning that traffic between different VSYSs cannot pass through the firewall by default. In this case, since the interfaces for each VSYS are assigned to separate virtual routers (VRs), and the desired traffic is still not passing between the two VSYSs, the firewall needs to be explicitly configured to allow traffic between them.

The required configuration is to add each VSYS to the list of visible virtual systems of the other VSYS. This allows inter-VSYS communication to be enabled, effectively permitting the traffic to pass between the zones of different VSYSs.

#### NEW QUESTION 49

.....

## 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/>