



# **Paloalto-Networks**

## **Exam Questions NGFW-Engineer**

Palo Alto Networks Next-Generation Firewall Engineer

#### NEW QUESTION 1

When configuring a Zone Protection profile, in which section (protection type) would an NGFW engineer configure options to protect against activities such as spoofed IP addresses and split handshake session establishment attempts?

- A. Flood Protection
- B. Protocol Protection
- C. Packet-Based Attack Protection
- D. Reconnaissance Protection

**Answer: B**

#### Explanation:

In the context of a Zone Protection profile, Protocol Protection is the section used to configure protections against activities such as spoofed IP addresses and split handshake session establishment attempts. These types of attacks typically involve manipulating protocol behaviors, such as IP address spoofing or session hijacking, and are mitigated by the Protocol Protection settings.

#### NEW QUESTION 2

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 3

Which zone type allows traffic between zones in different virtual systems (VSYS), without the traffic leaving the firewall?

- A. Isolated
- B. Transient
- C. External
- D. Internal

**Answer: B**

#### Explanation:

The Transient zone type is used to allow traffic between zones in different virtual systems (VSYS) on a Palo Alto Networks firewall without the traffic leaving the firewall. It provides a way for virtual systems to communicate with each other by acting as a temporary or intermediary zone. Traffic can pass through the firewall between the virtual systems without requiring physical interfaces or leaving the device.

#### NEW QUESTION 4

Which PAN-OS method of mapping users to IP addresses is the most reliable?

- A. Port mapping
- B. GlobalProtect
- C. Syslog
- D. Server monitoring

**Answer: D**

#### Explanation:

Server monitoring is the most reliable method for mapping users to IP addresses in PAN-OS. This method allows the firewall to monitor specific servers, such as Microsoft Active Directory (AD) or LDAP servers, to dynamically retrieve and update user-to-IP mappings. It provides a more accurate and up-to-date mapping of users to their associated IP addresses, as it directly queries user databases in real time.

#### NEW QUESTION 5

By default, which type of traffic is configured by service route configuration to use the management interface?

- A. Security zone
- B. IPSec tunnel
- C. Virtual system (VSYS)
- D. Autonomous Digital Experience Manager (ADEM)

**Answer: D**

#### Explanation:

By default, the Autonomous Digital Experience Manager (ADEM) traffic is configured to use the management interface in a Palo Alto Networks firewall. The management interface is typically used for management-related traffic, such as monitoring and logging, and it is configured to handle ADEM-related traffic for the optimal performance of digital experience monitoring features.

This default configuration helps ensure that ADEM traffic does not interfere with regular traffic that may traverse other interfaces, such as traffic from security zones or IPSec tunnels.

#### NEW QUESTION 6

Which interface types should be used to configure link monitoring for a high availability (HA) deployment on a Palo Alto Networks NGFW?

- A. HA, Virtual Wire, and Layer 2
- B. Tap, Virtual Wire, and Layer 3
- C. Virtual Wire, Layer 2, and Layer 3
- D. HA, Layer 2, and Layer 3

**Answer: C**

#### Explanation:

When configuring link monitoring for high availability (HA) on a Palo Alto Networks NGFW, the following interface types are supported:

Virtual Wire: Used when you have a transparent mode firewall deployment, where the firewall operates at Layer 2 to monitor traffic between two network segments.

Layer 2: Also used in transparent mode, where the firewall operates as a Layer 2 device and can be configured for link monitoring.

Layer 3: Used in routed mode, where the firewall is involved in routing traffic and can also be configured to monitor links.

#### NEW QUESTION 7

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 8

How does a Palo Alto Networks firewall choose the best route when it receives routes for the same destination from different routing protocols?

- A. The route that was received first will be entered into the forwarding table, and all subsequent routes will be rejected.
- B. It will attempt to load balance the traffic across all routes.
- C. It compares the administrative distance and chooses the one with the highest value.
- D. It compares the administrative distance and chooses the one with the lowest value.

**Answer: D**

#### Explanation:

When a Palo Alto Networks firewall receives routes for the same destination from different routing protocols, it uses the administrative distance (AD) to determine the best route. The administrative distance is a measure of the trustworthiness of a route, with a lower value indicating higher preference. The firewall will choose the route with the lowest administrative distance to populate its forwarding table.

#### NEW QUESTION 9

An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The application will be able to make any approved changes directly to devices via API.

What is a requirement for the application to create SD-WAN interfaces?

- A. REST API's `sdwanInterfaceprofiles` parameter on a Panorama device
- B. REST API's `sdwanInterfaces` parameter on a firewall device
- C. XML API's `sdwanprofiles/interfaces` parameter on a Panorama device
- D. XML API's `InterfaceProfiles/sdwan` parameter on a firewall device

**Answer: B**

#### Explanation:

To create SD-WAN interfaces through an API, the correct approach is to use the REST API's "sdwanInterfaces" parameter on a firewall device. This parameter allows you to configure SD-WAN interfaces directly on the firewall devices via API, ensuring that the required interfaces are set up and managed for SD-WAN functionality.

#### 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 10**

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 14**

A multinational organization wants to use the Cloud Identity Engine (CIE) to aggregate identity data from multiple sources (on premises AD, Azure AD, Okta) while enforcing strict data isolation for different regional business units. Each region's firewalls, managed via Panorama, must only receive the user and group information relevant to that region. The organization aims to minimize administrative overhead while meeting data sovereignty requirements.

Which approach achieves this segmentation of identity data?

- A. Create one CIE tenant, aggregate all identity data into a single view, and redistribute the full dataset to all firewall
- B. Rely on per-firewall Security policies to restrict access to out-of- scope user and group information.
- C. Establish separate CIE tenants for each business unit, integrating each tenant with the relevant identity source
- D. Redistribute user and group data from each tenant only to the region's firewalls, maintaining a strict one-to-one mapping of tenant to business unit.
- E. Disable redistribution of identity data entirel
- F. Instead, configure each regional firewall to pull user and group details directly from its local identity providers (IdPs).
- G. Deploy a single CIE tenant that collects all identity data, then configure segments within the tenant to filter and redistribute only the relevant user/group sets to each regional firewall group.

**Answer:** B

**Explanation:**

To meet the requirement of data isolation for different regional business units while minimizing administrative overhead, the best approach is to establish separate Cloud Identity Engine (CIE) tenants for each business unit. Each tenant would be integrated with the relevant identity sources (such as on-premises AD, Azure AD, and Okta) for that specific region. This ensures that the identity data for each region is kept isolated and only relevant user and group data is distributed to the respective regional firewalls.

By maintaining a strict one-to-one mapping between CIE tenants and business units, the organization ensures that each region's firewall only receives the user and group data relevant to that region, thus meeting data sovereignty requirements and minimizing administrative complexity.

**NEW QUESTION 15**

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 16**

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 17

In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.

What function do certificate profiles serve in this context?

- A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.
- B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for user or device authentication.
- C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.
- D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.

**Answer: B**

#### Explanation:

In the context of GlobalProtect with certificate-based authentication, certificate profiles are used to ensure proper validation of the certificates. They perform the following functions: Define trust anchors, which are the root and intermediate Certificate Authorities (CAs) that the firewall trusts to authenticate certificates. Specify revocation checks, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked.

Map certificate attributes, such as the Common Name (CN), which helps in authenticating users and devices based on their certificates.

#### NEW QUESTION 22

Which two statements describe an external zone in the context of virtual systems (VSYS) on a Palo Alto Networks firewall? (Choose two.)

- A. It is associated with an interface within a VSYS of a firewall.
- B. It is a security object associated with a specific virtual router of a VSYS.
- C. It is not associated with an interface; it is associated with a VSYS itself.
- D. It is a security object associated with a specific VSYS.

**Answer: AD**

#### Explanation:

In the context of virtual systems (VSYS) on a Palo Alto Networks firewall, the external zone is typically associated with specific interfaces within a VSYS. Zones are fundamental security objects used to define traffic flow between interfaces, and the external zone would be used for interfaces that connect to external networks.

An external zone is associated with an interface within a VSYS of the firewall. This ensures that traffic from specific interfaces can be classified as belonging to the external zone, allowing the firewall to apply appropriate security policies.

The external zone is indeed a security object that is specific to a given VSYS, as each VSYS can have its own set of zones that are isolated from others.

#### NEW QUESTION 26

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NGFW-Engineer Practice Exam Features:

- \* NGFW-Engineer Questions and Answers Updated Frequently
- \* NGFW-Engineer Practice Questions Verified by Expert Senior Certified Staff
- \* NGFW-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NGFW-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The NGFW-Engineer Practice Test Here](#)