



Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer

NEW QUESTION 1

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 2

Which configuration step is required when implementing a new self-signed root certificate authority (CA) certificate for SSL decryption on a Palo Alto Networks firewall?

- A. Import the new subordinate CA certificate into the trust stores of all client devices.
- B. Set the subordinate CA certificate as the default routing certificate for all network traffic.
- C. Configure the subordinate CA to issue certificates with indefinite validity periods.
- D. Disable all existing SSL decryption rules until the new certificate is fully propagated.

Answer: A

Explanation:

When implementing a new self-signed root certificate authority (CA) for SSL decryption on a Palo Alto Networks firewall, the subordinate CA certificate (which is generated by the firewall) must be imported into the trust stores of all client devices. This ensures that client devices trust the firewall as a valid certificate authority, enabling the firewall to decrypt and re-encrypt SSL traffic.

Importing the subordinate CA certificate into the client devices' trust stores is necessary for those devices to trust the new self-signed root CA and properly handle SSL decryption traffic.

NEW QUESTION 3

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 4

What must be configured before a firewall administrator can define policy rules based on users and groups?

- A. User Mapping profile
- B. Authentication profile
- C. Group mapping settings
- D. LDAP Server profile

Answer: C

Explanation:

Before a firewall administrator can define policy rules based on users and groups, the Group Mapping settings must be configured. These settings enable the firewall to map users to their respective Active Directory (AD) groups. This mapping allows the firewall to use user and group information to create policy rules based on group membership.

NEW QUESTION 5

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 6

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 7

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 8

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 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

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 10

.....

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](#)