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
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 3
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 4
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 5
A large enterprise wants to implement certificate-based authentication for both users and devices, using an on-premises Microsoft Active Directory Certificate Services (AD CS) hierarchy as the primary certificate authority (CA). The enterprise also requires Online Certificate Status Protocol (OCSP) checks to ensure efficient revocation status updates and reduce the overhead on its NGFWs. The environment includes multiple Active Directory forests, Panorama management for several geographically dispersed firewalls, GlobalProtect portals and gateways needing distinct certificate profiles for users and devices, and strict Security policies demanding frequent revocation checks with minimal latency.
Which approach best addresses these requirements while maintaining consistent policy enforcement?

A. Deploy self-signed certificates at each site to simplify local certificate validation and reduce dependencies on a centralized C
B. Turn off certificate revocation checks for lower overhead, rely on IP-based rules for GlobalProtect authentication, and use a single certificate profile for both users and devices.
C. Distribute the root and intermediate CA certificates via Panorama as shared objects to ensure all firewalls have a consistent trust chai
D. Configure OCSP responder profiles oneach firewall to offload revocation checks to an internal OCSP server while keeping CRL checks as a fallbac
E. Maintain separate certificate profiles for user and device authentication and use an automated enrollment method – such as Group Policy or SCEP – to deploy certificates to endpoints.

F. Configure each firewall independently to trust the root and intermediate CA certificate
G. Rely only on manual CRL checks for certificate revocation, and import both user and device certificates directly into each firewall??s local certificate store for authentication.
H. Obtain wildcard certificates from a public CA for both user and device authentication, and configure firewalls to perform CRL polling at the default update interva
I. Manually install user certificates on endpoints and synchronize firewall certificate stores through frequent manual SSH updates to maintain consistency.

Answer: B

Explanation:
This approach best addresses the enterprise??s requirements for certificate-based authentication, OCSP checks, and consistent policy enforcement:
Distributing the root and intermediate CA certificates via Panorama ensures that all firewalls in the enterprise are consistent in their trust chain and can validate certificates properly.
Configuring OCSP responder profiles on each firewall offloads the revocation checks to an internal OCSP server, which reduces the overhead on the firewalls and ensures fast, real- time certificate status checks.
Using CRL checks as a fallback ensures reliability in case the OCSP responder is unavailable.
Separate certificate profiles for users and devices ensure that the firewall can enforce different security policies based on the type of certificate (user vs. device).
Automated certificate enrollment methods such as Group Policy or SCEP streamline certificate distribution to endpoints, ensuring efficient management of certificates across geographically dispersed firewalls.

NEW QUESTION 6
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 7
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 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 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 10
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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