

NGFW-Engineer Dumps

Palo Alto Networks Next-Generation Firewall Engineer

<https://www.certleader.com/NGFW-Engineer-dumps.html>



NEW QUESTION 1

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 only
- 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 security
- D. Synchronize partial policy information into Panorama manually as needed.
- E. Use Kubernetes-native deployment tools (e.g., Helm) to deploy CN-Series in each cluster, 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 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

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 14

An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logout stage and SAML-based multi-factor authentication (MFA) for user login.

How does the GlobalProtect agent process the authentication flow on Windows endpoints?

- A. The GlobalProtect agent uses the machine certificate to establish a pre-logout tunnel; upon user sign-in, it prompts for SAML-based MFA credentials, ensuring both device and user identities are validated before granting full access.
- B. The GlobalProtect agent uses the machine certificate during pre-logout for initial tunnel establishment, and then seamlessly reuses the same machine certificate for user-based authentication without requiring MFA.
- C. Once the machine certificate is validated at pre-logout, the Windows endpoint completes MFA on behalf of the user by passing existing Windows Credential Provider details to the GlobalProtect gateway without prompting the user.
- D. GlobalProtect requires the user to log in first for SAML-based MFA before establishing the pre-logout tunnel, rendering the pre-logout certificate authentication (CA) flow redundant.

Answer: A

Explanation:

In a hybrid authentication model with both certificate-based authentication for pre-logout and SAML-based multi-factor authentication (MFA) for user login, the GlobalProtect agent processes the flow as follows:

During the pre-logout stage, the agent uses the machine certificate to authenticate and establish the initial VPN tunnel.

Once the user logs in (after the machine is connected), the agent then triggers SAML-based MFA to ensure the user is authenticated with multi-factor authentication, validating both the device and the user identity before granting full access.

This method ensures that both the device and user are properly authenticated and validated in the hybrid authentication model.

NEW QUESTION 16

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 20

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 24

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

What are the phases of the Palo Alto Networks AI Runtime Security: Network Intercept solution?

- A. Scanning, Isolation, Whitelisting, Logging
- B. Discovery, Deployment, Detection, Prevention
- C. Policy Generation, Discovery, Enforcement, Logging
- D. Profiling, Policy Generation, Enforcement, Reporting

Answer: B

Explanation:

The phases of the Palo Alto Networks AI Runtime Security: Network Intercept solution are designed to help identify and protect against potential threats in real time by using AI to detect and prevent malicious activities within the network.

Discovery: Identifying applications, services, and behaviors within the network to understand baseline activity.

Deployment: Implementing the solution into the network and integrating with existing security measures.

Detection: Monitoring traffic and activities to identify abnormal or malicious behavior. Prevention: Taking action to stop threats once detected, such as blocking malicious traffic or stopping exploit attempts.

NEW QUESTION 30

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 31

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 36

To maintain security efficacy of its public cloud resources by using native tools, a company purchases Cloud NGFW credits to replicate the Panorama, PA-Series, and VM-Series devices used in physical data centers. Resources exist on AWS and Azure:

The AWS deployment is architected with AWS Transit Gateway, to which all resources connect

The Azure deployment is architected with each application independently routing traffic. The engineer deploying Cloud NGFW in these two cloud environments must account for the following:

Minimize changes to the two cloud environments

Scale to the demands of the applications while using the least amount of compute resources

Allow the company to unify the Security policies across all protected areas. Which two implementations will meet these requirements? (Choose two.)

- A. Deploy a VM-Series firewall in AWS in each VPC, create an IPSec tunnel between AWS and Azure, and manage the policy with Panorama.
- B. Deploy Cloud NGFW for Azure in vNET/s, update the vNET/s routing to path traffic through the deployed NGFWs, and manage the policy with Panorama.
- C. Deploy Cloud NGFW for Azure in vWAN, create a vWAN to route all appropriate traffic to the Cloud NGFW attached to the vWAN, and manage the policy with local rules.
- D. Deploy Cloud NGFW for AWS in a centralized Security VPC, update the Transit Gateway to route all appropriate traffic through the Security VPC, and manage the policy with Panorama.

Answer: BD

Explanation:

To meet the company's requirements - minimizing changes to the cloud environments, optimizing compute resources, and unifying security policies - the best approach is to deploy Cloud NGFW solutions natively for AWS and Azure while managing policies centrally with Panorama.

In Azure, using Cloud NGFW for Azure deployed within vNETs allows traffic to be routed through security appliances efficiently without requiring a complete re-architecture. This approach aligns with Azure's existing routing mechanism while maintaining security.

In AWS, deploying Cloud NGFW for AWS in a centralized Security VPC and integrating it with AWS Transit Gateway enables traffic inspection for all connected VPCs without modifying individual workloads. This method ensures efficient scaling and minimal infrastructure changes while maintaining security consistency.

NEW QUESTION 41

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 42

Which forwarding methods can be used on the Objects tab when configuring the Log Forwarding profile?

- A. Panorama, syslog, email
- B. Syslog, HTTP, NetFlow
- C. Panorama, ADEM, syslog
- D. SNMP, HTTP, RADIUS

Answer: A

Explanation:

When configuring the Log Forwarding profile on a Palo Alto Networks firewall, the forwarding methods available include:

Panorama: For forwarding logs to a Panorama management system. Syslog: For forwarding logs to a syslog server.

Email: For sending logs via email.

NEW QUESTION 47

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 50

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NGFW-Engineer Exam with Our Prep Materials Via below:

<https://www.certleader.com/NGFW-Engineer-dumps.html>