PaloAltoNetworks.NGFW-Engineer.v2026-04-28.q29

Exam Code:	NGFW-Engineer
Exam Name:	Palo Alto Networks Next-Generation Firewall Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	29
Version:	v2026-04-28
# of views:	105
# of Questions views:	290
https://www.freepdfdumps.com/PaloAltoNetworks.NGFW-Engineer.v2026-04-28.q29.html	

NEW QUESTION: 1
Why is SSL/TLS decryption considered critical for effective NGFW security inspection in modern networks?
A. It reduces network latency
B. It eliminates the need for IPS
C. It enables inspection of encrypted application traffic
D. It simplifies firewall rule design
Answer: C (LEAVE A REPLY)
Most modern traffic is encrypted.
SSL/TLS decryption allows NGFWs to inspect traffic content and detect threats hidden within encrypted sessions.

NEW QUESTION: 2
How does a Palo Alto firewall handle traffic between two different security zones?
A. Traffic between zones is forwarded without inspection
B. Traffic is allowed automatically between zones
C. Traffic is denied by default unless a security policy explicitly allows it
D. Traffic is automatically encrypted between zones
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
After upgrading PAN-OS, which action is recommended to ensure that all features function correctly?
A. Verify and, if necessary, update content and application signatures.
B. Disable and re-enable all interfaces.
C. Reset all configurations to default.

D. Reboot the firewall multiple times.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
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: A,B (LEAVE A REPLY)
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: 5
How do Zone Protection Profiles enhance network security?
A. By replacing security policies with predefined rule sets
B. By dynamically assigning users to security groups
C. By providing protection against flood attacks, reconnaissance scans, and packet-based threats
D. By encrypting all traffic entering and leaving the zone
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
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 (LEAVE A REPLY)
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: 7
A security team wants to block peer-to-peer file sharing applications even when those applications attempt to evade detection by using non-standard ports.
Which NGFW capability enables this control?
A. Port-based access control
B. Application signature and behavior analysis
C. Static access control lists
D. QoS traffic shaping
Answer: B (LEAVE A REPLY)
NGFWs analyze traffic patterns and application signatures, allowing them to detect and block applications regardless of port usage.

NEW QUESTION: 8
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: (SHOW ANSWER)
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: 9

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: C (LEAVE A REPLY)

Packet-Based Attack Protection examines IP, TCP, ICMP, IPv6, and ICMPv6 packet headers to drop packets with undesirable characteristics like IP spoofing or malformed TCP options that enable split handshakes.

NEW QUESTION: 10

An organization wants to protect its internal network from previously unknown malware that does not match any existing signatures.

Which NGFW feature BEST addresses this requirement?

A. Stateful inspection

B. Intrusion Prevention System (IPS)

C. URL filtering

D. Sandbox / Advanced Threat Protection

Answer: (SHOW ANSWER)

Sandboxing executes suspicious files in an isolated environment and analyzes their behavior, making it effective against zero-day threats.

NEW QUESTION: 11

Which set of options is available for detailed logs when building a custom report on a Palo Alto Networks NGFW?

A. Traffic, User-ID, URL

B. Traffic, threat, data filtering, User-ID

C. GlobalProtect, traffic, application statistics

D. Threat, GlobalProtect, application statistics, WildFire submissions

Answer: (SHOW ANSWER)

When building a custom report on a Palo Alto Networks NGFW, you can select detailed logs that provide specific insights into various aspects of firewall activity. The available options for detailed logs typically include:

Traffic logs: These provide information on the network traffic passing through the firewall.

Threat logs: These logs capture data related to identified security threats, such as malware or intrusion attempts.

Data filtering logs: These logs capture events related to data filtering policies, such as preventing the transfer of sensitive data.

User-ID logs: These logs associate user identities with the traffic and activities observed on the firewall, enabling user-based policy enforcement.

NEW QUESTION: 12
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 (LEAVE A REPLY)
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: 13
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: (SHOW ANSWER)
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: 14
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 (LEAVE A REPLY)
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: 15
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 (LEAVE A REPLY)
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: 16
In an authentication sequence, what happens if the "Continue on client cert failure" option is enabled?
A. The firewall will prompt the user to provide a valid client certificate.
B. The firewall will skip client certificate authentication and proceed to the next authentication profile in the sequence.
C. The firewall will deny access if the client certificate is invalid.
D. The firewall will log the failure and terminate the session.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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: (SHOW ANSWER)
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: 18
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: B,D (LEAVE A REPLY)
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: 19
What is the function of a Certificate Revocation List (CRL) in a PKI?
A. Lists certificates that have been revoked before their expiration date
B. Lists certificates pending renewal
C. Lists expired certificates
D. Lists all issued certificates
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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 (LEAVE A REPLY)
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: 21
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: (SHOW ANSWER)
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: 22
An NGFW is deployed inline to inspect traffic without requiring any changes to existing IP addressing or routing configurations.
Which deployment mode is being used?

A. Layer 3 routed mode
B. Layer 2 switching mode
C. Virtual Wire / transparent mode
D. VPN mode
Answer: C (LEAVE A REPLY)
Virtual Wire (transparent) mode allows the NGFW to inspect traffic without modifying the network topology.

NEW QUESTION: 23
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 (LEAVE A REPLY)
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: 24
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: (SHOW ANSWER)
The HA3 interface, a Layer 2 link using MAC-in-MAC encapsulation, enables packet forwarding between active/active firewalls to handle asymmetric routing and ensure proper session setup when traffic arrives at the non-owner peer.

NEW QUESTION: 25
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 (LEAVE A REPLY)
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: 26
An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logon stage and SAML-based multi-factor authentication (MFA) for user logon.
How does the GlobalProtect agent process the authentication flow on Windows endpoints?
A. The GlobalProtect agent uses the machine certificate to establish a pre-logon 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-logon 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-logon, 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-logon tunnel, rendering the pre-logon certificate authentication (CA) flow redundant.
Answer: A (LEAVE A REPLY)
In a hybrid authentication model with both certificate-based authentication for pre-logon and SAML-based multi-factor authentication (MFA) for user logon, the GlobalProtect agent processes the flow as follows:
During the pre-logon 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: 27

What is a key difference between OSPF and BGP when used in a Palo Alto Networks firewall?
A. OSPF is used for internal routing, while BGP is primarily used for external routing
B. OSPF is faster than BGP in all scenarios
C. OSPF operates only on IPv6, while BGP is for IPv4
D. BGP does not require neighbor relationships, while OSPF does
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
In a Collector Group with multiple Log Collectors, enabling redundancy ensures that:
A. Each log has two copies, each residing on a different Log Collector.
B. Logs are distributed based on a round-robin mechanism.
C. Logs are stored in a compressed format to save space.
D. Each log is stored only on the primary Log Collector.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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: (SHOW ANSWER)
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.

Valid NGFW-Engineer Dumps shared by Actual4test.com for Helping Passing NGFW-Engineer Exam! Actual4test.com now offer the **newest NGFW-Engineer exam dumps**, the Actual4test.com NGFW-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NGFW-Engineer dumps with Test Engine here: https://www.actual4test.com/NGFW-Engineer_examcollection.html (**128** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)