NGFW-Engineer Official Study Guide - NGFW-Engineer Valid Real Test

www.nwexam.com PDF

b) By replacing security policies with predefined rule sets
c) By encrypting all traffic entering and leaving the zone
d) By dynamically assigning users to security groups
Answer: a

03. After upgrading PAN-OS, which action is recommended to ensure that all features function correctly?
a) Reboot the firewall multiple times.
b) Reset all configurations to default.
c) Verify and, if necessary, update content and application signatures.
d) Disable and re-enable all interfaces.
Answer: c

04. In an authentication sequence, what happens if the "Continue on client cert failure" option is enabled?
a) The firewall will skip client certificate authentication and proceed to the next authentication profile in the sequence.
b) The firewall will deny access if the client certificate is invalid.
c) The firewall will prompt the user to provide a valid client certificate.
d) The firewall will log the failure and terminate the session.
Answer: a

05. Before upgrading a Palo Alto Networks firewall to a new PAN-OS version, which preliminary step is crucial to ensure a smooth upgrade process?
a) Disable all security policies.
b) Back up the current configuration.
c) Reset the firewall to factory settings.
d) Disable High Availability (HA) if configured.
Answer: b

06. How does a Palo Alto firewall handle traffic between two different security zones?
a) Traffic is denied by default unless a security policy explicitly allows it
b) Traffic is allowed automatically between zones
c) Traffic is automatically encrypted between zones
d) Traffic between zones is forwarded without inspection
Answer: a

07. For explicit proxy deployment, which port is typically used by the client browsers to send requests to the proxy?

NGFW-Engineer Sample Questions 5

What's more, part of that Itcerttest NGFW-Engineer dumps now are free: https://drive.google.com/open?id=1dgBpY8roQENBSx-pmdHnZhYAerSaJVxe

Itcerttest NGFW-Engineer products are honored by thousands, considerably recognized across the industry. Successful candidates preferably suggest our products as they provide the best possible returns for your invested money. Our professionals have devoted themselves to deliver the required level of efficiency for our customers. Our well repute in industry highlights our tremendous success record and makes us incomparable choice for NGFW-Engineer Exams preparation. 100% guaranteed success for all NGFW-Engineer exams is offered at Itcerttest, marks key difference with competing brands. Your investment with Itcerttest never takes any down turn as we owe the whole responsibility for any kind of loss that occurs through your failure.

Palo Alto Networks NGFW-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Integration and Automation: This section measures the skills of Automation Engineers in deploying and managing Palo Alto Networks NGFWs across various environments. It includes the installation of PA-Series, VM-Series, CN-Series, and Cloud NGFWs. The use of APIs for automation, integration with third-party services like Kubernetes and Terraform, centralized management with Panorama templates and device groups, as well as building custom dashboards and reports in Application Command Center (ACC) are key topics.

Topic 2	• PAN-OS Networking Configuration: This section of the exam measures the skills of Network Engineers in configuring networking components within PAN-OS. It covers interface setup across Layer 2, Layer 3, virtual wire, tunnel interfaces, and aggregate Ethernet configurations. Additionally, it includes zone creation, high availability configurations (active • active and active • passive), routing protocols, and GlobalProtect setup for portals, gateways, authentication, and tunneling. The section also addresses IPSec, quantum-resistant cryptography, and GRE tunnels.
Topic 3	• PAN-OS Device Setting Configuration: This section evaluates the expertise of System Administrators in configuring device settings on PAN-OS. It includes implementing authentication roles and profiles, and configuring virtual systems with interfaces, zones, routers, and inter-VSYS security. Logging mechanisms such as Strata Logging Service and log forwarding are covered alongside software updates and certificate management for PKI integration and decryption. The section also focuses on configuring Cloud Identity Engine User-ID features and web proxy settings.

NGFW-Engineer Valid Real Test - Test NGFW-Engineer Pdf

The Palo Alto Networks NGFW-Engineer exam offers a great opportunity for beginner and experienced to validate their expertise in a short time period. To do this they just need to pass the Palo Alto Networks Next-Generation Firewall Engineer NGFW-Engineer Certification Exam which is not an easy task. And Itcerttest offfers latest NGFW-Engineer exam practice, exam pattern and practice exam online.

Palo Alto Networks Next-Generation Firewall Engineer Sample Questions (Q124-Q129):

NEW QUESTION # 124
An NGFW engineer is configuring multiple Panorama-managed firewalls to start sending all logs to Strata Logging Service. The Strata Logging Service instance has been provisioned, the required device certificates have been installed, and Panorama and the firewalls have been successfully onboarded to Strata Logging Service.
Which configuration task must be performed to start sending the logs to Strata Logging Service and continue forwarding them to the Panorama log collectors as well?

- A. Enable the "Panorama/Cloud Logging" option in the Logging and Reporting Settings section under Device --> Setup --> Management in the appropriate templates.
- B. Select the "Enable Cloud Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.
- C. Select the "Enable Duplicate Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.
- D. Modify all active Log Forwarding profiles to select the "Cloud Logging" option in each profile match list in the appropriate device groups.

Answer: B

Explanation:
To begin sending logs to Strata Logging Service while continuing to forward them to Panorama log collectors, the necessary configuration is to enable Cloud Logging. This option is configured in the Cloud Logging section under Device # Setup # Management in the appropriate templates. Once enabled, this ensures that logs are directed both to the Strata Logging Service (cloud) and to the Panorama log collectors.

NEW QUESTION # 125
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 an authentication sequence that includes both the "RADIUS" Server Profile and "SAML Identity Provider" Server Profile to run the two services in tandem.
- B. Create and add the "SAML Identity Provider" Server Profile to the authentication profile for the "RADIUS" Server Profile.
- C. Create a testing and rollback plan for the transition from Radius to SAML, as the two authentication profiles cannot be run in tandem.
- D. Create and apply an authentication profile with the "SAML Identity Provider" Server Profile.

Answer: A,B

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 # 126
A network architect is planning the deployment of a new IPSec VPN tunnel to connect a local data center to a cloud environment. The plan must include all necessary Security policy configurations for both tunnel negotiation and data transit.
Which two Security policy requirements must be included in the implementation plan? (Choose two.)

- A. A pair of policies is required to control the flow of data traffic into and out of the security zone assigned to the tunnel interface.
- B. The default interzone-default security policy is sufficient to allow the tunnel negotiation traffic between the firewall and the remote peer.
- C. A policy must explicitly permit the IPSec container application between the external-facing zone and local zone.
- D. A policy must explicitly permit only the IKE application between the external-facing zone and local zone.

Answer: A,D

Explanation:
IKE negotiation traffic must be explicitly permitted between the external-facing zone and the local zone so the tunnel can be established, and separate Security policy rules are required to control the actual user/data traffic entering and leaving the zone assigned to the tunnel interface to enforce what can traverse the VPN.

NEW QUESTION # 127
What is a valid configurable limit for setting resource quotas when defining a new VSYS on a Palo Alto Networks firewall?

- A. Maximum number of SSL decryption rules
- B. Maximum number of virtual routers
- C. Disk space allocation for logs
- D. Percentage of total CPU utilization

Answer: A

Explanation:
When defining a new VSYS, PAN-OS allows administrators to set explicit resource quotas on policy-related objects, including limits on rule capacities, which can include SSL decryption rules as part of security policy resources, enabling controlled allocation of configuration and processing capacity per VSYS.

NEW QUESTION # 128
Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?

- A. LLDP
- B. Link Duplex

- C. DDNS
- D. NetFlow

Answer: D

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 # 129
.....

Our NGFW-Engineer study braindumps are comprehensive that include all knowledge you need to learn necessary knowledge, as well as cope with the test ahead of you. With convenient access to our website, you can have an experimental look of free demos before get your favorite NGFW-Engineer prep guide downloaded. You can both learn useful knowledge and pass the exam with efficiency with our NGFW-Engineer Real Questions easily. We are on the way of meeting our mission and purposes of helping exam candidates to consider the exam as a campaign of success and pass the exam successfully.