NetSec-Analyst유효한인증덤프최신버전덤프공부자료

BONUS!!! Pass4Test NetSec-Analyst 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1Ba-C4Mp_EMNwVgO9WEawBh4Ef1TUFCcX

Palo Alto Networks NetSec-Analyst시험패스는 어려운 일이 아닙니다. Pass4Test의 Palo Alto Networks NetSec-Analyst 덤프로 시험을 쉽게 패스한 분이 헤아릴수 없을 만큼 많습니다. Palo Alto Networks NetSec-Analyst덤프의 데모를 다운받아 보시면 구매결정이 훨씬 쉬워질것입니다. 하루 빨리 덤프를 받아서 시험패스하고 자격증 따보세요.

Palo Alto Networks NetSec-Analyst 시험요강:

주제	소개
주제 1	• Management and Operations: This section of the exam measures the skills of Security Operations Professionals and covers the use of centralized management tools to maintain and monitor firewall environments. It focuses on Strata Cloud Manager, folders, snippets, automations, variables, and logging services. Candidates are also tested on using Command Center, Activity Insights, Policy Optimizer, Log Viewer, and incident-handling tools to analyze security data and improve the organization overall security posture. The goal is to validate competence in managing day-to-day firewall operations and responding to alerts effectively.

주제 2	• Troubleshooting: This section of the exam measures the skills of Technical Support Analysts and covers the identification and resolution of configuration and operational issues. It includes troubleshooting misconfigurations, runtime errors, commit and push issues, device health concerns, and resource usage problems. This domain ensures candidates can analyze failures across management systems and on-device functions, enabling them to maintain a stable and reliable security infrastructure.
주제 3	• Policy Creation and Application: This section of the exam measures the abilities of Firewall Administrators and focuses on creating and applying different types of policies essential to secure and manage traffic. The domain includes security policies incorporating App-ID, User-ID, and Content-ID, as well as NAT, decryption, application override, and policy-based forwarding policies. It also covers SD-WAN routing and SLA policies that influence how traffic flows across distributed environments. The section ensures professionals can design and implement policy structures that support secure, efficient network operations.
주제 4	• Object Configuration Creation and Application: This section of the exam measures the skills of Network Security Analysts and covers the creation, configuration, and application of objects used across security environments. It focuses on building and applying various security profiles, decryption profiles, custom objects, external dynamic lists, and log forwarding profiles. Candidates are expected to understand how data security, IoT security, DoS protection, and SD-WAN profiles integrate into firewall operations. The objective of this domain is to ensure analysts can configure the foundational elements required to protect and optimize network security using Strata Cloud Manager.

적중율 높은 NetSec-Analyst유효한 인증덤프 덤프자료

Palo Alto Networks인증NetSec-Analyst시험을 위하여 최고의 선택이 필요합니다. Pass4Test 선택으로 좋은 성적도 얻고 하면서 저희 선택을 후회하지 않을것니다.돈은 적게 들고 효과는 아주 좋습니다.우리Pass4Test여러분의 응시분비에 많은 도움이 될뿐만아니라Palo Alto Networks인증NetSec-Analyst시험은 또 일년무료 업데이트서비스를 제공합니다.작은 돈을 투자하고 이렇게 좋은 성과는 아주 바람직하다고 봅니다.

최신 Network Security Administrator NetSec-Analyst 무료샘플문제 (Q187-Q192):

질문 # 187
How many zones can an interface be assigned with a Palo Alto Networks firewall?

- A. two
- B. three
- C. four
- D. one

정답： D

설명：
References:

질문 # 188
Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

- A. Group Mapping
- B. IP User
- C. Valid Username Detected Log Severity
- D. Domain Credential

정답： D

설명:
Domain Credential detection is the User Credential Detection method that checks for the submission of a valid corporate username and the associated password within a URL Filtering Security profile. This method requires the Windows User-ID agent and the User-ID credential service to be installed on a read-only domain controller (RODC). The firewall can then detect passwords submitted to web pages and compare them with the domain credentials stored on the RODC. If the firewall detects a match, it can block the request, alert the user, or generate a log entry1. Reference: Configure Credential Detection with the Windows User-ID Agent, Set Up Credential Phishing Prevention, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

질문 # 189
A cybersecurity firm manages multiple tenants on a single Palo Alto Networks firewall using Virtual Systems (vSys). Each vSys has its own PBF policies. A new requirement dictates that all outbound web traffic (TCP/80, 443) from a specific subnet (172.16.0.0/24) in 'vSys_A' must first be directed to an external web proxy (192.0.2.254) before being sent to the internet. This proxy is located in a different vSys, 'vSys_B', which has a dedicated interface (ethernet1/10) for this proxy integration. All other traffic from 172.16.0.0/24 in 'vSys A' should follow its regular internet path. Which PBF configuration is appropriate, and what critical inter-vSys element is needed?

- A. This scenario requires a dedicated physical interface to connect 'vSys_A' to 'vSys_B' as an 'inter-vSys' data plane link, and PBF cannot be used to directly forward traffic between Virtual Systems.
- B. In 'vSys_A', create a PBF rule: Source Address: 172.16.0.0/24, Application: web-browsing, ssl, Action: Forward, Egress Interface: (Inter-vSys Link Interface), Next Hop: 192.0.2.254. An 'Inter-vSys Link' must be configured between 'vSys_A' and 'vSys_B'.
- C. In 'vSys_A', create a PBF rule: Source Address: 172.16.0.0/24, Application: web-browsing, ssl, Action: Forward, Virtual Router: (Virtual Router in vSys_B), Next Hop: 192.0.2.254. This requires an inter-vSys forwarding mechanism to be configured.
- D. In 'vSys_A', create a PBF rule: Source Address: 172.16.0.0/24, Application: web-browsing, ssl, Action: Forward, Virtual Router: (Virtual Router in vSys_B where the proxy's network resides). In 'vSys_B', a static route for 172.16.0.0/24 must point to the proxy via ethernet1/10.
- E. In 'vSys_A', create a PBF rule: Source Address: 172.16.0.0/24, Application: web-browsing, ssl, Egress Interface: ethernet1/10 (assigned to vSys_B), Next Hop: 192.0.2.254, Action: Forward. Ensure a security policy exists in vSys_B to allow traffic from vSys_A to the proxy.

정답: B

설명:
This is a complex inter-vSys PBF scenario. Palo Alto Networks firewalls can forward traffic between Virtual Systems using a special configuration called an 'Inter-vSys Link'. This is a logical link, not a physical one, that allows traffic from one vSys to be forwarded to another. Inter-vSys Link (Critical Element): An 'Inter-vSys Link' must be configured under 'Network > Virtual Wires' or 'Network > Interfaces' (depending on the PAN-OS version and desired setup). This link creates a logical connection between two Virtual Routers across different vSystems. One end is attached to a Virtual Router in 'vSys_A', and the other to a Virtual Router in 'vSys_B'. PBF Rule: In 'vSys_A', the PBF rule will then specify the 'Egress Interface' as the 'Inter-vSys Link Interface' that connects to 'vSys_B'. The 'Next Hop' would be the IP address of the proxy (192.0.2.254), which is assumed to be reachable via 'vSys_B'. Let's evaluate other options: Option A: A PBF rule in 'vSys_A' cannot directly specify an egress interface that belongs to 'vSys_B'. They are isolated routing domains. Option B and D: The 'Virtual Router' action in PBF is for transferring traffic between Virtual Routers within the same Virtual System . It cannot transfer traffic between different Virtual Systems directly. Option E: This is incorrect. While dedicated physical links can be used, the 'Inter-vSys Link' feature is designed for logical forwarding between vSystems without consuming additional physical interfaces for simple transfers like this.

질문 # 190
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

- A. interzone
- B. universal
- C. intrazone
- D. global

정답: A

설명:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of%20availability

질문 # 191
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

- A. It defines the SSUTLS encryption strength used to protect the management interface.
- B. It defines the certificate to send to the client's browser from the management interface.
- C. It defines the firewall's global SSL/TLS timeout values.
- D. It defines the CA certificate used to verify the client's browser.

정답: B

질문 # 192
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes