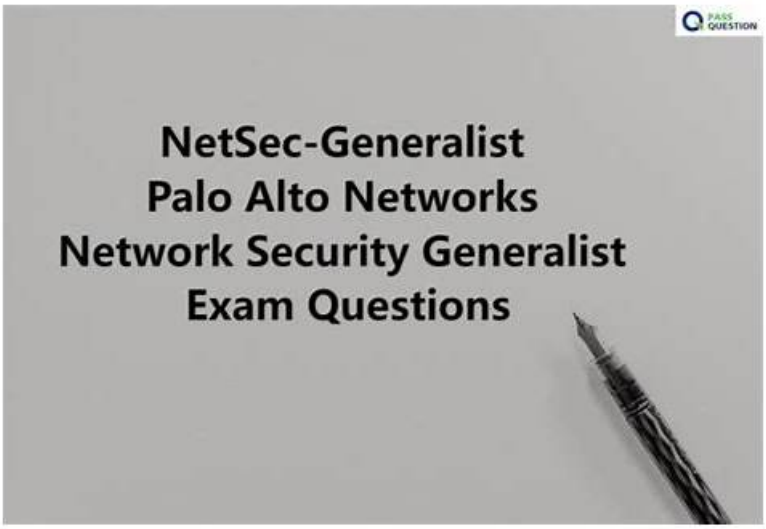
NetSec-Generalist Practice Test: Palo Alto Networks Network Security Generalist & NetSec-Generalist Exam Preparation & NetSec-Generalist Study Guide



DOWNLOAD the newest TestkingPass NetSec-Generalist PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ejnoXtIyK8TnQ9I6os5f3aZOiRqrU2N0

Unlike other NetSec-Generalist study materials, there is only one version and it is not easy to carry. Our NetSec-Generalist exam questions mainly have three versions which are PDF, Software and APP online, and for their different advantafes, you can learn anywhere at any time. And the prices of our NetSec-Generalist training engine are reasonable for even students to afford and according to the version that you want to buy.

Palo Alto Networks NetSec-Generalist Exam Syllabus Topics:

Topic	Details
Topic 1	• Connectivity and Security: This section targets Network Managers in maintaining • configuring network security across on-premises • cloud • hybrid networks by focusing on network segmentation strategies along with implementing secure policies • certificates to protect connectivity points within these environments effectively. A critical skill assessed is segmenting networks securely to prevent unauthorized access risks.
Topic 2	• Platform Solutions, Services, and Tools: This section measures the skills of IT Architects in describing Palo Alto Networks NGFW and Prisma SASE products for enhanced security efficacy. It covers creating security policies with User-ID • App-ID configurations along with monitoring tools like CDSS (Cloud-Delivered Security Services). A key skill measured is configuring cloud-delivered services efficiently.
Topic 3	• Infrastructure Management and CDSS: This section measures the skills of Infrastructure Managers in managing CDSS infrastructure by configuring profiles • policies for IoT devices or enterprise DLP • SaaS security solutions while ensuring data encryption • access control practices are implemented correctly across these platforms. A key skill measured is securing IoT devices through proper configuration.
Topic 4	• NGFW and SASE Solution Functionality: This section targets Cybersecurity Specialists to understand the functionality of Cloud NGFWs, PA-Series, CN-Series, and VM-Series firewalls. It includes perimeter security, zone segmentation, high availability configurations, security policy implementation, and monitoring • logging practices. A critical skill assessed is implementing zone security policies effectively.

Topic 5	• Network Security Fundamentals: This section measures the skills of Network Security Engineers and explains application layer inspection for Strata and SASE products. It covers topics such as slow path versus fast path packet inspection, decryption methods like SSL Forward Proxy, and network hardening techniques including Content and Zero Trust. A key skill measured is applying decryption techniques effectively.

>> Valid NetSec-Generalist Cram Materials <<

NetSec-Generalist Study Questions are Most Powerful Weapon to Help You Pass the Palo Alto Networks Network Security Generalist exam - TestkingPass

In this rapid rhythm society, the competitions among talents are growing with each passing day, some job might ask more than one's academic knowledge it might also require the professional NetSec-Generalistcertification and so on. It can't be denied that professional certification is an efficient way for employees to show their personal Palo Alto Networks Network Security Generalist abilities. In order to get more chances, more and more people tend to add shining points, for example a certification to their resumes. Passing exam won't be a problem anymore as long as you are familiar with our NetSec-Generalist Exam Material (only about 20 to 30 hours practice). High accuracy and high quality are the reasons why you should choose us.

Palo Alto Networks Network Security Generalist Sample Questions (Q18-Q23):

NEW QUESTION # 18
Which firewall attribute can an engineer use to simplify rule creation and automatically adapt to changes in server roles or security posture based on log events?

- A. Dynamic Address Groups
- B. Dynamic User Groups
- C. Predefined IP addresses
- D. Address objects

Answer: A

NEW QUESTION # 19
A hospital system allows mobile medical imaging trailers to connect directly to the internal network of its various campuses. The network security team is concerned about this direct connection and wants to begin implementing a Zero Trust approach in the flat network.
Which solution provides cost-effective network segmentation and security enforcement in this scenario?

- A. Deploy edge firewalls at each campus entry point to monitor and control various traffic types through direct connection with the trailers.
- B. Manually inspect large images like holograms and MRIs, but permit smaller images to pass freely through the campus core firewalls.
- C. Configure access control lists on the campus core switches to control and inspect traffic based on image size, type, and frequency.
- D. Configure separate zones to isolate the imaging trailer's traffic and apply enforcement using the existing campus core firewalls.

Answer: D

Explanation:
In a Zero Trust Architecture (ZTA), network segmentation is critical to prevent unauthorized lateral movement within a flat network. Since the hospital system allows mobile medical imaging trailers to connect directly to its internal network, this poses a significant security risk, as these trailers may introduce malware, vulnerabilities, or unauthorized access to sensitive medical data.
The most cost-effective and practical solution in this scenario is:

Creating separate security zones for the imaging trailers.
Applying access control and inspection policies via the hospital's existing core firewalls instead of deploying new hardware.
Implementing strict policy enforcement to ensure that only authorized communication occurs between the trailers and the hospital's network.
Why Separate Zones with Enforcement is the Best Solution?
Network Segmentation for Zero Trust
By placing the medical imaging trailers in their own firewall-enforced zone, they are isolated from the main hospital network.
This reduces attack surface and prevents an infected trailer from spreading malware to critical hospital systems.
Granular security policies ensure only necessary communications occur between zones.
Cost-Effective Approach
Uses existing core firewalls instead of deploying costly additional edge firewalls at every campus.
Reduces complexity by leveraging the current security infrastructure.
Visibility & Security Enforcement
The firewall enforces security policies, such as allowing only medical imaging protocols while blocking unauthorized traffic.
Integration with Threat Prevention and WildFire ensures that malicious files or traffic anomalies are detected.
Logging and monitoring via Panorama helps the security team track and respond to threats effectively.
Other Answer Choices Analysis
(A) Deploy edge firewalls at each campus entry point
This is an expensive approach, requiring multiple hardware firewalls at every hospital location.
While effective, it is not the most cost-efficient solution when existing core firewalls can enforce the necessary segmentation and policies.
(B) Manually inspect large images like holograms and MRIs
This does not align with Zero Trust principles.
Manual inspection is impractical, as it slows down medical workflows.
Threats do not depend on image size; malware can be embedded in small and large files alike.
(D) Configure access control lists (ACLs) on core switches
ACLs are limited in security enforcement, as they operate at Layer 3/4 and do not provide deep inspection (e.g., malware scanning, user authentication, or Zero Trust enforcement).
Firewalls offer application-layer visibility, which ACLs on switches cannot provide.
Switches do not log and analyze threats like firewalls do.
Reference and Justification:
Firewall Deployment - Firewall-enforced network segmentation is a key practice in Zero Trust.
Security Policies - Granular policies ensure medical imaging traffic is controlled and monitored.
VPN Configurations - If remote trailers are involved, secure VPN access can be enforced within the zones.
Threat Prevention & WildFire - Firewalls can scan imaging files (e.g., DICOM images) for malware.
Panorama - Centralized visibility into all traffic between hospital zones and trailers.
Zero Trust Architectures - This solution follows Zero Trust principles by segmenting untrusted devices and enforcing least privilege access.
Thus, Configuring separate zones (C) is the correct answer, as it provides cost-effective segmentation, Zero Trust enforcement, and security visibility using existing firewall infrastructure.

NEW QUESTION # 20
All branch sites in an organization have NGFWs running in production, and the organization wants to centralize its logs with Strata Logging Service.
Which type of certificate is required to ensure connectivity from the NGFWs to Strata Logging Service?

- A. Intermediate CA
- B. Device
- C. Root
- D. Server

Answer: B

NEW QUESTION # 21
A company currently uses Prisma Access for its mobile users. A use case is discovered in which mobile users will need to access an internal site, but there is no existing network communication between the mobile users and the internal site.
Which Prisma Access functionality needs to be deployed to enable routing between the mobile users and the internal site?

- A. Interconnect license
- B. Autonomous Digital Experience Manager (ADEM)
- C. Security processing node
- D. Service connection

Answer: D

Explanation:
Prisma Access provides secure remote access for mobile users, but by default, mobile users cannot access internal sites unless explicitly configured.
How Service Connection Enables Routing Between Mobile Users and Internal Sites:
Service Connection establishes a secure tunnel between Prisma Access and the internal network.
Allows direct routing between mobile users and internal applications.
Enables access without requiring additional VPN connections.
Ensures that Prisma Access can securely route traffic between mobile users and the internal site.
Why Other Options Are Incorrect?
A . Interconnect license □
Interconnect provides higher bandwidth connections between Prisma Access and multiple regions, but it does not create routing to internal networks.
C . Autonomous Digital Experience Manager (ADEM) □
ADEM is used for network experience monitoring, not for routing or connectivity.
D . Security Processing Node □
Security processing nodes handle threat inspection, but they do not create routing connections between Prisma Access and internal networks.
Reference to Firewall Deployment and Security Features:
Firewall Deployment - Service connections extend internal network access.
Security Policies - Enforces policies on traffic between mobile users and internal resources.
VPN Configurations - Ensures secure IPsec/GRE tunnels between Prisma Access and on-prem networks.
Threat Prevention - Inspects mobile-to-internal traffic for threats.
WildFire Integration - Scans transferred files between mobile users and internal sites.
Zero Trust Architectures - Ensures secure access control for mobile users accessing internal applications.
Thus, the correct answer is:
□ B. Service connection

NEW QUESTION # 22
Why would an enterprise architect use a Zero Trust Network Access (ZTNA) connector instead of a service connection for private application access?

- A. It controls traffic from the mobile endpoint to any of the organization's internal resources.
- B. It supports traffic sourced from on-premises or public cloud-based resources to mobile users and remote networks.
- C. It functions as the attachment point for IPSec-based connections to remote site or branch networks.
- D. It automatically discovers private applications and suggests Security policy rules for them.

Answer: D

Explanation:
A Zero Trust Network Access (ZTNA) connector is used instead of a service connection for private application access because it provides automatic application discovery and policy enforcement.
Why is ZTNA Connector the Right Choice?
Discovers Private Applications
The ZTNA connector automatically identifies previously unknown or unmanaged private applications running in a data center or cloud environment.
Suggests Security Policy Rules
After discovering applications, it suggests appropriate security policies to control user access, ensuring Zero Trust principles are followed.
Granular Access Control
It enforces least-privilege access and applies identity-based security policies for private applications.
Other Answer Choices Analysis
(A) Controls traffic from the mobile endpoint to any of the organization's internal resources This describes ZTNA enforcement, but does not explain why a ZTNA connector is preferred over a service connection.

(B) Functions as the attachment point for IPsec-based connections to remote site or branch networks This describes a service connection, which is different from a ZTNA connector.
(C) Supports traffic sourced from on-premises or public cloud-based resources to mobile users and remote networks This aligns more with Prisma Access service connections, not ZTNA connectors.
Reference and Justification:
Zero Trust Architectures - ZTNA ensures that private applications are discovered, classified, and protected.
Firewall Deployment & Security Policies - ZTNA connectors automate private application security.
Threat Prevention & WildFire - Provides additional security layers for private apps.
Thus, ZTNA Connector (D) is the correct answer, as it automatically discovers private applications and suggests security policy rules for them.

NEW QUESTION # 23
.....