PAN-OS Network Security Architect Training

OEM: Palo Alto • Duration: 4 Days (32 hrs) • Code: PCNSA-ARCH

COURSE MODULES & TOPICS

Domain 1: Zero Trust Enterprise (8%)

- User-ID, Device Health, HIP, Security Posture, and Device-ID Controls
- Network Segmentation vs Microsegmentation
- Application Access Differentiation
- Continuous Security Scanning
- Continuous Monitoring and Analytics

Domain 2: AI Security (11%)

- Prisma AIRS and AI Access: AI Red Teaming, Model Scanning, Runtime Security, AI Agents
- Kubernetes Integration and Microsegmentation
- App-ID Cloud Engine, Advanced Threat Prevention, Advanced URL Filtering, Enterprise DLP
- Standard AI Security Architectures
- AI Application Classification and Security Controls
- AI Security Frameworks

Domain 3: Centralized Management and IAM (13%)

- Panorama and Log Collectors: HA and Resilience/Redundancy
- Strata Cloud Manager (SCM), Strata Logging Service, Cloud Identity Engine
- Directory Sync: On-Premises Agent, Cloud Directory, SAML 2.0
- Strata Logging Service Log Forwarding
- User Identification and Authentication
- Cloud Identity Engine Use Cases: NGFW, Prisma Access, Prisma SD-WAN

Domain 4: SSE Private Application Access (11%)

- Prisma Access Regional and Global Deployments
- On-Ramp and Off-Ramp Architectures
- ZTNA Connectors
- Colo-Connect and NCC (Network Cloud Connector)
- Private App Access Through Prisma Browser

Domain 5: Mobile User Security (7%)

- Prisma Browser, Prisma Access Agent, Explicit Proxy, and GlobalProtect Use Cases
- GlobalProtect Connection Methods: On-Demand, User-Logon Always On, Pre-Logon Always On
- Prisma Access Mobile Users
- ADEM (Autonomous Digital Experience Management) Design

Domain 6: Modernizing Branches (11%)

- Branch Architectures for SASE/HA: Prisma Access Remote Networks, Prisma SD-WAN, PAN-OS SD-WAN, ADEM, Third-Party Edge/SD-WAN
- Advanced Security for Prisma SD-WAN: App-ID, Device-ID, User-ID
- Threat Prevention, URL Filtering, and DNS Security for SD-WAN Branches

Domain 7: Data Security (7%)

- SaaS Security Inline vs SaaS API Security (In-Motion Inline, At-Rest API, SSPM)
- SaaS Application Usage Control
- Enterprise DLP Classifiers: Traditional/Regex, EDM, IDM, OCR, ML Classification
- Endpoint DLP and Policy-Based DLP

Domain 8: Securing IoT Environments (11%)

- Device Security Architecture: Visibility/Discovery/Risk Assessment, Enforcement
- IoT Sensor Placement Options
- Visibility Functionality: NGFW, Virtual Metadata Collector, Prisma SD-WAN, PAN-OS SD-WAN
- Device-ID Capabilities
- Device Security Capabilities

Domain 9: Public Cloud (11%)

- NGFW Integrations: AWS, Azure, GCP, OCI
- Maintenance and Security Across Cloud Service Providers
- AWS NGFW: GWLB, Transit Gateway, HA, Subinterfaces
- Azure NGFW: Insertion Options, Load Balancer, HA
- GCP NGFW: Insertion Options, Load Balancer, HA
- VM-Series vs Cloud NGFW Solutions

Domain 10: Private Cloud (10%)

- Capacity Requirements: Edge, Core, East-West Microsegmentation
- VM-Series Across Hypervisors: AHV, KVM, ESXi
- SSL Decryption vs Performance Trade-offs
- HA Deployment: Active/Passive, Active/Active, Hardware Firewall Clustering (HSF), Fast Failover
- Layer 3 Routing: ECMP, Static, BGP, OSPF
- Systems Management, New Hardware Deployment, and SSL Inspection Sizing