COURSE TABLE OF CONTENTS

PAN-OS Network Security Professional Training

OEM: Palo Alto • Duration: 5 Days (40 hrs) • Code: PCCNSP

COURSE MODULES & TOPICS

Domain 1: Network Security Fundamentals (17%)

- Application Layer Inspection
- Slow Path vs Fast Path Processing
- Decryption: SSL Forward Proxy, SSL Inbound Inspection, SSH Proxy
- Network Hardening Methods: Content-ID, Zero Trust, User-ID, Device-ID, Zones

Domain 2: NGFW and SASE Solution Functionality (13%)

- Cloud NGFWs, PA-Series, CN-Series, VM-Series
- Prisma SD-WAN
- Prisma Access
- Panorama and Strata Cloud Manager (SCM)

Domain 3: Platform Solutions, Services, and Tools (30%)

- Security Efficacy
- Cloud-Delivered Security Services (CDSS): IoT Security, Enterprise DLP, SaaS Security, PAN-OS SD-WAN, Premium GlobalProtect
- Advanced WildFire, Advanced Threat Prevention (ATP), Advanced URL Filtering, Advanced DNS Security
- AIOps for NGFW
- Next-Generation Technical Support (NGTS)
- Quantum Security Risks
- AI Security Risks

Domain 4: NGFW and SASE Solution Maintenance and Configuration (10%)

- Hardware, VM-Series, CN-Series, and Cloud NGFW Configuration & Maintenance
- Prisma Access Configuration & Maintenance

Domain 5: Infrastructure Management and CDSS (17%)

- Security Policies, Profiles, and Updates in CDSS
- IoT Security and Device-IDs
- Enterprise DLP and SaaS Security: Data Encryption, Access Control

- SCM and Panorama Management

Domain 6: Connectivity and Security (13%)

- On-Premises, Cloud, and Hybrid Network Security
- Remote User Connectivity and Security