

# **Palo Alto Networks Certified Network Security Engineer (PCNSE) Training**

*COURSE CONTENT*

## **GET IN TOUCH**



Multisoft Systems  
B - 125, Sector - 2, Noida



(+91) 9810-306-956



info@multisoftsystems.com



www.multisoftsystems.com

## About Multisoft

---

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

## About Course

---

The Palo Alto Networks Certified Network Security Engineer (PCNSE) training offered by Multisoft Systems is a detailed program designed to equip IT professionals with advanced knowledge and technical expertise in Palo Alto Networks' security platform. This training's aim to develop proficiency in implementing, managing, and troubleshooting Palo Alto Networks solutions, focusing on the latest cybersecurity technologies and best practices.

## Module 1: Introduction

- ✓ Next Generation Firewall Features - APP-ID, User-ID, Content-ID, Decryption
- ✓ Port Based Vs Application FW
- ✓ SP3 Architecture of Palo Alto
- ✓ Hardware and VM models
- ✓ Firewall GUI and CLI Tour

## Module 2: Initial Config and Traffic Forwarding

- ✓ Initial Configuration and Deployment modes
- ✓ Register the firewall and licensing
- ✓ Segmenting using Interface and zone Configuration
- ✓ Layer-2, Layer-3, Virtual Wire and TAP Deployment modes
- ✓ Objects: address, Service, Application, Groups and filters
- ✓ Setup Basic Security Policies
- ✓ Routing Configuration using Virtual Router
- ✓ Configuring Basic NAT Rules
- ✓ Basic Traffic Monitoring

## Module 3: Firewall Administration

- ✓ Management Interfaces
- ✓ Configuration management, Commit, Export, Backup Revert
- ✓ Manage Firewall Administrators
- ✓ Content Upgrades, PANOS Upgrades
- ✓ Service Route Configuration

## Module 4: Policies

- ✓ Policy Types
- ✓ Security Policies
- ✓ NAT Rules, Source and Destination NATS

- ✓ QoS Policies
- ✓ Decryption Policies
- ✓ DOS and Zone Protection
- ✓ Security Profiles

## **Module 5: Application Identification and Decryption**

- ✓ APPID Feature of the Firewall
- ✓ Applications, Groups and Filters
- ✓ Application Override and Custom Application
- ✓ APP-ID Based Policies
- ✓ SSL/TLS Protocol
- ✓ SSL/TLS Decryption
- ✓ SSL Forward Proxy, Inbound inspection and SSH proxy
- ✓ Certificate management for decryption

## **Module 6: Traffic Forwarding and Troubleshooting**

- ✓ Palo Alto Packet Flow
- ✓ Netting Issues, Routing or Policy issues
- ✓ Session Setup and Session monitoring
- ✓ Packet Capture
- ✓ Traffic Flows
- ✓ TCP vs UDP Traffic
- ✓ Flow Basic Logs
- ✓ Troubleshooting Traffic issues and Wireshark analysis of Packets

## **Module 7: Authentication and USER-ID**

- ✓ Authentication and Types
- ✓ Local and LDAP Based Authentication
- ✓ User-ID Concepts
- ✓ Group Mappings and User Mappings

- ✓ Agentless and Agent Based User-ID configuration
- ✓ Configure User and Group Based Policies

## **Module 8: Content Inspection**

- ✓ Antivirus Profiles
- ✓ Anti-Spyware Profiles
- ✓ Vulnerability Protection
- ✓ URL Filtering Concepts
- ✓ PAN-DB Categorization
- ✓ Custom URL Categories
- ✓ Create Exceptions
- ✓ File Blocking
- ✓ Wild Fire

## **Module 9: High-Availability**

- ✓ Active/Passive and Active/Active Scenarios
- ✓ Active/Passive Configuration
- ✓ Failover testing
- ✓ Link and Path Monitoring
- ✓ Troubleshooting Failover Issues

## **Module 10: VPN Configurations**

- ✓ Site-Site VPN
- ✓ Route based and Policy Based VPNs
- ✓ Global Protect
- ✓ GP Gateway and Portals
- ✓ On-Demand, Pre-login modes of Global Protect