Palo Alto Networks Firewall Training

Hands-On Next-Generation Firewall Administration | Aligned to PCNSA Exam Objectives

Course Description

The Palo Alto Networks Firewall Training at Zoom Technologies is a complete, hands-on program that takes you from network security fundamentals to confident administration of Palo Alto Next-Generation Firewalls — the industry's leading enterprise security platform. Starting with firewall essentials and Palo Alto's Single-Pass Parallel Processing (SP3) architecture, you'll configure every major capability live in a virtual lab you build yourself on VMware Workstation: zones and interfaces, routing, NAT, security policies, App-ID™, Content-ID™ threat prevention (Antivirus, Anti-Spyware, URL Filtering, WildFire™), User-ID™, SSL decryption, IPSec Site-to-Site VPN, and log monitoring. By the end, you'll be able to deploy, configure, secure, and troubleshoot a Palo Alto NGFW in a real enterprise environment — with a curriculum closely mapped to the PCNSA certification exam objectives.

Who Should Attend

This course is designed for anyone who wants to build or advance a career in network security using the industry's leading NGFW platform:

- **Network & Security Engineers** who manage firewalls (Cisco ASA, FortiGate, SonicWall, Sophos, Check Point) and want to add Palo Alto skills to their profile
- **System / Network Administrators** responsible for perimeter security, VPNs, and secure Internet access in their organizations
- **SOC Analysts & Security Operations Teams** who investigate firewall logs and alerts and want to understand how policies, App-ID, and threat prevention actually work
- **Fresh Graduates & Career Changers** with basic networking knowledge (routing, switching, TCP/IP) aiming for high-demand firewall administrator roles
- **PCNSA / PCNSE Aspirants** preparing for Palo Alto Networks certification exams
- **IT Managers & Consultants** who design, recommend, or audit network security solutions for clients

Prerequisites

Basic understanding of TCP/IP, IP addressing, and routing concepts (CCNA-level knowledge is helpful but not mandatory). No prior firewall experience is required — the course starts from firewall fundamentals.

Key Topics You Will Master

- **NGFW Fundamentals**
- **Palo Alto Architecture (SP3)**
- **Complete Lab Build on VMware**
- **Zones, Interfaces & Routing**
- **NAT in Depth**
- **Security Policies**
- **Content-ID™ Threat Prevention**
- **SSL Decryption**
- **App-ID™**
- **User-ID™**
- **IPSec Site-to-Site VPN**
- **Log Monitoring**

Detailed Course Content

Module 1: Network Security Fundamentals

- Network security technologies — where firewalls fit in the security stack
- Firewall vs. Next-Generation Firewall — roles in a layered defense

Module 2: Firewalls

- What is a firewall — how traffic filtering actually works
- Types of firewalls — packet filtering, stateful inspection, proxy/application-layer
- Designing network security with firewalls — perimeter, DMZ, and segmentation design

Module 3: Next-Generation Firewalls (NGFW)

- What is a next-generation firewall
- Difference between a traditional firewall and an NGFW — application awareness, integrated IPS, user identity, and threat intelligence

Module 4: Introduction to Palo Alto Networks

- What is Palo Alto — platform overview and market position
- Palo Alto packet flow — the life of a packet through the firewall
- Single-Pass Parallel Processing (SP3) architecture — why one scan beats many
- Control Plane and Data Plane — management vs. traffic processing

Module 5: Deploying Palo Alto in a Lab (Hands-On)

- Importing the Palo Alto VM into VMware Workstation
- Setting up the lab environment and configuring VMware virtual network adapters
- Mapping virtual network adapters to Palo Alto network interfaces

Module 6: Initial Configuration

- Configuring the management interface and first-time login to the GUI dashboard
- Hostname, timezone, NTP, DHCP, DNS, and DNS Cache Proxy configuration
- Service route configuration — controlling which interface handles which service

Module 7: Zones & Interfaces

- Inside and Outside security zones — the foundation of every policy
- Interface deployment modes: Layer 2, Layer 3, TAP, and Virtual Wire

Module 8: Routing

- Virtual routers — the routing engine inside the firewall
  - Default routing for Internet-bound traffic
  - Static routes for internal and branch networks

Module 9: Network Address Translation (NAT)

- Dynamic NAT
- Dynamic IP & Port NAT (Source NAT / PAT) — many users, one public IP
- Static NAT — one-to-one mapping for published servers
- Destination NAT (port redirection) — publishing internal services securely

Module 10: Security Policies

- Building the security rulebase — zones, addresses, applications, services, actions

- Policy ordering, shadowing, and best practices for a clean rulebase

Module 11: Content-ID™ — Threat Prevention

- Antivirus profiles — blocking malware in real time
- Anti-Spyware profiles — detecting command-and-control (C2) traffic
- Vulnerability Protection — integrated IPS against exploits
- URL Filtering — Palo Alto categories and custom URL groups
- File Blocking and WildFire™ — stopping malicious files and zero-day analysis in the cloud sandbox
- Data Filtering — preventing sensitive data leakage
- Zone Protection — defending against reconnaissance and floods
- DoS Protection — safeguarding critical servers from denial-of-service attacks

> ***Note:*** *Hands-on practice of the Content-ID™ topics above (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering — Palo Alto Categories & Custom URL Groups, File Blocking & WildFire™, Data Filtering, Zone Protection, and DoS Protection) requires an active Palo Alto Networks license/subscription on the firewall.*

Module 12: SSL Inspection (Decryption)

- Generating and deploying trusted certificates
- Configuring decryption policies to inspect HTTPS/SSL traffic

Module 13: App-ID™ — Application Identification

- The App-ID process — how the firewall identifies applications regardless of port or protocol
- Building application-based security policies

Module 14: User-ID™ — Identity-Based Control

- Local user authentication
- User-ID Agent deployment
- LDAP / Active Directory integration
- Captive Portal for unidentified users

Module 15: VPN

- IPSec Site-to-Site VPN — phase 1 & phase 2 configuration, tunnel interfaces, and verification

Module 16: Log Monitoring

- Traffic, Threat, URL, and System logs — reading, filtering, and investigating
- Using logs for day-to-day operations, troubleshooting, and incident response

Why Learn Palo Alto at Zoom Technologies

- **100% hands-on labs —** you build and keep your own Palo Alto virtual lab from day one
- **Real-world scenarios —** training delivered by practicing security professionals, not just slides
- **Certification-focused —** curriculum aligned to PCNSA exam objectives
- **Trusted since 1996 —** 300,000+ professionals trained across networking, security, and cloud
- **Career pathway —** combine with our SOC Analyst and Cybersecurity Professional programs for a complete security skill set