ZOOM
TECHNOLOGIES

Palo Alto Firewall Training

(Hands-On Next-Generation Firewall Administration)

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.

Key Topics:

- 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

+91 7893399822 priya@zoomgroup.com www.zoomgroup.com

Palo Alto Firewall Training

Module 1: Network Security Fundamentals

- Network security technologies
- Firewall vs. Next-Generation Firewall

Module 2: Firewalls

- What is a firewall
- Types of firewalls
- Designing network security with firewalls

Module 3: Next-Generation Firewalls (NGFW)

- What is a next-generation firewall
- Difference between a traditional firewall and an NGFW

Module 4: Introduction to Palo Alto Networks

- What is Palo Alto
- Palo Alto packet flow
- Single-Pass Parallel Processing (SP3) architecture
- Control Plane and Data Plane

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, time zone, NTP, DHCP, DNS, and DNS Cache Proxy configuration
- Service route configuration

Module 7: Zones & Interfaces

- Inside and Outside security zones
- Interface deployment modes: Layer 2, Layer 3, TAP, and Virtual Wire

Module 8: Routing

- Virtual routers
- 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)
- Static NAT
- Destination NAT (port redirection)

Module 10: Security Policies

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

Module 11: Content-ID — Threat Prevention

- Antivirus profiles
- Anti-Spyware profiles
- Vulnerability Protection
- URL Filtering
- File Blocking and WildFire
- Data Filtering
- Zone Protection
- DoS Protection

Palo Alto Firewall Training

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
- 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

Module 16: Log Monitoring

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