Palo Alto Networks Firewall Administration & Security

12 – 16 September 2027
Amman (Jordan)



Palo Alto Networks Firewall Administration & Security

Ref: 3256006_358552 **Date:** 12 – 16 September 2027 **Location:** Amman (Jordan) **Fees:** 4900 GBP

Introduction

This one-week specialized course provides participants with a comprehensive understanding of **Palo Alto Networks Next-Generation Firewalls and PAN-OS**. It focuses on firewall architecture, security policies, network protection, threat prevention, VPN security, centralized management, monitoring, and troubleshooting concepts.

The course is designed for IT and cybersecurity professionals who need to understand how Palo Alto Networks firewalls are structured, managed, secured, and optimized within enterprise environments. The program is delivered by one specialized trainer to ensure consistency and continuity throughout the training.

Course Objectives

By the end of this course, participants will be able to:

- Understand Palo Alto Networks firewall architecture and PAN-OS.
- Explain firewall interfaces, security zones, and routing concepts.
- Understand Security Policies and NAT.
- Explain Application-ID and User-ID.
- Understand Security Profiles and threat prevention.
- Understand GlobalProtect VPN architecture.
- Understand Panorama and centralized firewall management.
- Analyze firewall logs and security events.
- Understand High Availability concepts.
- Identify common firewall issues and troubleshooting approaches.
- Apply Palo Alto security best practices.

Course Outline

Day 1: Palo Alto Networks & PAN-OS Fundamentals



- Introduction to Palo Alto Networks Next-Generation Firewalls.
- Palo Alto firewall architecture.
- Overview of PAN-OS.
- Firewall interfaces and Security Zones.
- Virtual routers and routing concepts.
- Network segmentation.
- Administrative access and device management.
- Configuration and policy management concepts.

Day 2: Security Policies, NAT & Application Control

- Security Policy architecture.
- Security rules and policy evaluation.
- Address and service objects.
- Source NAT and Destination NAT.
- Application-ID concepts.
- Application-based security policies.
- User-ID concepts.
- User-based security policies.
- Security policy optimization and best practices.

Day 3: Threat Prevention & GlobalProtect

- Security Profiles and Profile Groups.
- Anti-Virus and Anti-Spyware protection.
- Vulnerability Protection.
- URL Filtering.
- WildFire and threat intelligence concepts.
- SSL/TLS security concepts.
- GlobalProtect architecture.
- Remote-access VPN concepts.
- GlobalProtect security and best practices.

Day 4: Monitoring, Panorama & High Availability



- Palo Alto logging architecture.
- Traffic, Threat, URL, and System logs.
- Security event monitoring and analysis.
- Firewall performance monitoring.
- Panorama architecture and centralized management.
- Device Groups and Templates.
- Centralized policy management.
- High Availability concepts.
- Active/Passive HA architecture.
- Monitoring and failover considerations.

Day 5: Troubleshooting, Optimization & Security Operations

- Palo Alto troubleshooting methodology.
- Connectivity and routing troubleshooting concepts.
- Security Policy and NAT troubleshooting.
- Application-ID and User-ID troubleshooting.
- GlobalProtect troubleshooting concepts.
- Log analysis and security event investigation.
- Firewall performance optimization.
- Security hardening and best practices.
- Common configuration issues.
- Final course review and discussion.

Why Attend This Course? Wins & Losses!

Wins

- Build a strong understanding of Palo Alto Networks firewalls.
- Develop knowledge of PAN-OS administration and security concepts.
- Understand enterprise firewall policies and network protection.
- Strengthen knowledge of threat prevention and security monitoring.
- Understand GlobalProtect and Panorama.
- Improve firewall troubleshooting and optimization knowledge.
- Apply Palo Alto security best practices.

Losses

Without proper knowledge of Palo Alto firewall technologies, organizations may face:



- Poorly designed security policies.
- Limited visibility into network activity.
- Increased security risks.
- Inefficient firewall management.
- Longer troubleshooting and incident-response times.

Conclusion

This course provides a focused theoretical understanding of **Palo Alto Networks Next-Generation Firewalls and PAN-OS**, covering administration, security policies, threat prevention, VPN, centralized management, monitoring, and troubleshooting.

Delivered by one specialized trainer, the program provides a consistent and structured learning experience for professionals seeking to strengthen their knowledge of Palo Alto security technologies.

Frequently Asked Questions FAQ

Who should attend this course?
Network Engineers, Network Administrators, Cybersecurity Professionals, Firewall Administrators, and IT Security Officers.

Is previous Palo Alto experience required?
No. Basic networking and cybersecurity knowledge is recommended.

Is the course practical?
No. This version is designed as **theory-based instructor-led training**.

Does the course cover PAN-OS?
Yes. PAN-OS is one of the core topics of the program.

Does the course cover GlobalProtect and Panorama?
Yes. Both are covered from an architectural, administrative, and security perspective.

