

EDU-210 Palo Alto Firewall Training: Configuration and Management

30 November – 4 December 2026
London

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

EDU-210 Palo Alto Firewall Training: Configuration and Management

Ref: 103600672_229737 **Date:** 30 November – 4 December 2026 **Location:** London **Fees:** 5700 Euro

Course Overview:

EDU-210 is a one-week Palo Alto Firewall Training program designed to build practical capability in configuring, managing, securing, and monitoring Palo Alto Networks next-generation firewalls. The course is particularly relevant to professionals working in communications operations, network support, infrastructure, security operations, and technical service delivery environments such as CommOps/RTSD, where secure connectivity, network availability, policy enforcement, and operational visibility are critical.

The course follows the technical scope of Palo Alto Networks Firewall Essentials: Configuration and Management, covering firewall architecture, initial configuration, administrator accounts, production network connectivity, Palo Alto Security Zones, Palo Alto Security Policy, Palo Alto NAT Policy, Palo Alto App-ID, Palo Alto User-ID, Palo Alto Security Profiles, Palo Alto URL Filtering, Palo Alto WildFire, decryption, and Palo Alto Firewall Logging and Reporting.

This Palo Alto Networks Training course combines Firewall Configuration Training, Firewall Management Training, Network Security Training, and practical NGFW Training. Participants learn how to apply Palo Alto Firewall Configuration and Management principles to approved network traffic, threat prevention, application control, user-based access, encrypted traffic, and network monitoring. The supporting materials also extend the learning into Palo Alto GlobalProtect, Palo Alto High Availability, Palo Alto VPN Configuration, and zone protection.

AGILE LEADERS
Training Center

Target Audience:

- CommOps / RTSD Professionals
- Network Engineers
- Network Security Engineers
- Security Engineers
- Security Administrators
- Security Operations Specialists
- Network Operations Engineers
- Infrastructure Engineers
- Firewall Administrators
- Network Support Engineers
- Security Analysts
- Technical Support Staff
- IT Infrastructure Specialists
- Telecommunications Network Specialists
- System and Network Administrators

Targeted Organizational Departments:

- Network Operations and Communications Operations
- RTSD / Technical Service Delivery
- Cybersecurity and Information Security
- Security Operations Center
- Network Engineering
- IT Infrastructure
- Telecommunications Operations
- Enterprise Technology
- Network Support and Maintenance
- Technical Operations
- Infrastructure Security
- IT Operations

AGILE LEADERS
Training Center

Targeted Industries:

- Telecommunications
- Oil and Gas
- Energy and Utilities
- Government and Public Sector
- Banking and Financial Services
- Aviation and Airports
- Transportation and Logistics
- Critical Infrastructure
- Technology and Data Centers
- Defense and Security
- Industrial and Manufacturing
- Healthcare
- Large Corporate Enterprises
- Managed Network and Security Service Providers

Course Offerings:

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

- Explain Palo Alto Networks next-generation firewall architecture and the role of PAN-OS.
- Perform essential Palo Alto Firewall Configuration and initial management tasks.
- Configure firewall administrator accounts and appropriate administrative access.
- Connect a firewall securely to production environments using Palo Alto Security Zones.
- Create, organize, and manage Palo Alto Security Policy rules.
- Configure and manage Palo Alto NAT Policy rules for approved network connectivity.
- Apply Palo Alto App-ID to identify and control application usage.
- Configure Palo Alto Security Profiles for Palo Alto Threat Prevention.
- Apply Palo Alto URL Filtering to control inappropriate or risky web traffic.
- Use Palo Alto WildFire concepts to address unknown threats.
- Implement Palo Alto User-ID to control access according to user identity.
- Understand decryption controls for identifying threats within encrypted traffic.
- Interpret traffic, threat, and system information using Palo Alto Firewall Logging and Reporting.
- Understand the operational role of Palo Alto GlobalProtect for endpoint and remote access security.
- Explain Palo Alto High Availability concepts for firewall redundancy.
- Understand Palo Alto VPN Configuration for secure remote-site connectivity.
- Apply Firewall Management Training principles to operational troubleshooting and policy review.
- Strengthen enterprise network protection through practical Next Generation Firewall Training.

These outcomes reflect the official EDU-210 objectives of configuring and managing essential NGFW functions, Security and NAT policies, Threat Prevention strategies, and network traffic monitoring.

AGILE LEADERS
Training Center

Training Methodology:

EDU-210 uses a practical, instructor-led methodology that combines technical explanation, guided configuration, operational scenarios, structured demonstrations, group discussion, and hands-on lab-style activities. The source material specifically defines the course format as lecture and hands-on labs, with participants gaining practical experience configuring, managing, and monitoring a Palo Alto Networks firewall.

Each major technical concept is introduced through a short technical briefing before participants examine how the feature is applied in a production network. Palo Alto Firewall Configuration exercises focus on interfaces, zones, administrator accounts, Security Policy, NAT Policy, App-ID, User-ID, Security Profiles, URL Filtering, WildFire, decryption, and logging.

Scenario-based discussions are aligned with CommOps/RTSD responsibilities. Participants consider situations such as securing production connectivity, controlling access between network segments, allowing approved applications, troubleshooting blocked services, analyzing logs, maintaining firewall availability, and connecting remote sites securely.

The instructor uses configuration examples, policy walkthroughs, troubleshooting scenarios, network diagrams, and group analysis to reinforce Palo Alto Firewall Management principles. Guided feedback sessions allow participants to compare configuration choices and identify operational risks. Palo Alto GlobalProtect, Palo Alto High Availability, VPN connectivity, and Zone Protection are incorporated as supporting concepts to strengthen enterprise Firewall Configuration Training and Network Security Training.

AGILE LEADERS
Training Center

Course Toolbox:

- EDU-210 Course Reference Guide
- Palo Alto Firewall Architecture Reference
- PAN-OS Configuration Examples
- Palo Alto Security Zones Reference
- Security Policy Configuration Examples
- NAT Policy Configuration Examples
- App-ID Configuration Examples
- User-ID Configuration Examples
- Palo Alto Security Profiles Reference
- Threat Prevention Configuration Examples
- URL Filtering Examples
- WildFire Workflow Examples
- Decryption Policy Examples
- Firewall Logging and Reporting Examples
- GlobalProtect Architecture Examples
- High Availability Configuration Examples
- VPN Configuration Examples
- Zone Protection Examples
- Network Security Configuration Scenarios
- Firewall Troubleshooting Scenarios
- Policy Review Checklist
- Configuration Review Checklist
- Traffic and Threat Log Interpretation Guide

Note: Tools, commercial licenses, vendor subscriptions, Palo Alto Networks appliances, and software platforms are not provided as part of the course unless specifically agreed. Where relevant, the course provides technical insights, demonstrations, references, and examples of tools and platform features used in Palo Alto Firewall Administration.

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Palo Alto Firewall Architecture, Initial Configuration and Production Connectivity

- **Topic 1:** Palo Alto Networks Portfolio and Next-Generation Firewall Architecture
- **Topic 2:** PAN-OS Training Fundamentals and Firewall Management Interfaces
- **Topic 3:** Configuring Initial Palo Alto Firewall Settings
- **Topic 4:** Managing Palo Alto Firewall Configurations and Configuration Changes
- **Topic 5:** Managing Firewall Administrator Accounts and Administrative Access
- **Topic 6:** Connecting Palo Alto Firewalls to Production Networks with Security Zones
- **Reflection & Review:** Review firewall architecture, management access, configuration workflows, and Palo Alto Security Zones for CommOps/RTSD environments.

Day 2: Security Policy, NAT and Application Control

- **Topic 1:** Palo Alto Security Policy Fundamentals and Rule Processing
- **Topic 2:** Creating and Managing Security Policy Rules
- **Topic 3:** Palo Alto NAT Policy Concepts and Traffic Translation
- **Topic 4:** Creating and Managing NAT Policy Rules
- **Topic 5:** Controlling Application Usage with Palo Alto App-ID
- **Topic 6:** Applying Application-Based Access Controls to Production Networks
- **Reflection & Review:** Review Security Policy, NAT Policy, App-ID, zone relationships, and approved traffic flows.

AGILE LEADERS
Training Center

Day 3: Threat Prevention, Security Profiles, URL Filtering and WildFire

- **Topic 1:** Palo Alto Threat Prevention Concepts and Security Profile Strategy
- **Topic 2:** Blocking Known Threats Using Palo Alto Security Profiles
- **Topic 3:** Controlling Web Access with Palo Alto URL Filtering
- **Topic 4:** Identifying and Blocking Unknown Threats with Palo Alto WildFire
- **Topic 5:** Protecting Networks from Packet, Protocol and Known-Source Threats
- **Topic 6:** Applying Threat Prevention Controls to Enterprise and Operational Networks
- **Reflection & Review:** Review how Security Profiles, URL Filtering, WildFire, and Threat Prevention work together to reduce network exposure.

Day 4: User-ID, Decryption, Logging and Operational Monitoring

- **Topic 1:** Palo Alto User-ID Architecture and Identity-Based Security
- **Topic 2:** Controlling Network Resource Access with User-ID
- **Topic 3:** Configuring User-ID Windows Agent Concepts
- **Topic 4:** Using Decryption to Identify Threats in Encrypted Traffic
- **Topic 5:** Palo Alto Firewall Logging and Reporting
- **Topic 6:** Using Traffic and Threat Information for Firewall Troubleshooting
- **Reflection & Review:** Review identity-based access, encrypted traffic inspection, logging, reporting, and operational troubleshooting.

Day 5: GlobalProtect, High Availability, VPNs and Integrated Firewall Operations

- **Topic 1:** Palo Alto GlobalProtect for Secure Endpoint and Remote Access
- **Topic 2:** Palo Alto High Availability and Firewall Redundancy
- **Topic 3:** Palo Alto VPN Configuration for Remote-Site Connectivity
- **Topic 4:** Zone Protection and Common Network Attack Protection
- **Topic 5:** Integrated Palo Alto Firewall Administration and Operational Troubleshooting
- **Topic 6:** Applying EDU-210 Skills to CommOps/RTSD Network Operations
- **Reflection & Review:** Consolidate Security Policy, NAT, App-ID, User-ID, Threat Prevention, VPN, HA, logging, and operational firewall-management concepts.

AGILE LEADERS
Training Center

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should understand fundamental networking concepts, particularly routing, switching, and IP addressing, and should be familiar with basic network-security concepts. Previous exposure to IPS, proxies, content filtering, or other security technologies is useful but not mandatory. These prerequisites align directly with the EDU-210 source materials.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20-25 hours of instruction.

Is EDU-210 only about basic firewall configuration, or does it also cover advanced operational features?

EDU-210 begins with essential Palo Alto Firewall Configuration and Management but extends beyond basic setup. Participants work with Security Policy, NAT Policy, App-ID, Security Profiles, URL Filtering, WildFire, User-ID, decryption, logging, and reporting. Supporting EDU-210 materials also cover Palo Alto GlobalProtect, Palo Alto High Availability, VPN connectivity, and Zone Protection, providing broader operational context for enterprise firewall administration.

How This Course is Different from Other EDU-210 Courses:

This EDU-210 course maintains the technical structure of Palo Alto Networks Firewall Essentials while adapting the learning experience to corporate operational environments where network availability, communications continuity, controlled access, and rapid troubleshooting are essential. Rather than presenting Palo Alto Firewall Training as a sequence of isolated product features, the course connects Palo Alto Firewall Configuration and Management to real enterprise network operations.

Participants progress from firewall architecture and initial configuration into production connectivity, Palo Alto Security Zones, Palo Alto Security Policy, Palo Alto NAT Policy, App-ID, User-ID, Threat Prevention, Security Profiles, URL Filtering, WildFire, decryption, and Palo Alto Firewall Logging and Reporting. These areas closely reflect the official EDU-210 module structure.

The key distinction is the operational emphasis for CommOps/RTSD and similar technical roles. Configuration decisions are discussed in terms of service availability, network segmentation, secure application access, remote-site connectivity, traffic troubleshooting, and operational resilience.

The course also integrates supplemental areas including Palo Alto GlobalProtect, Palo Alto High Availability, Palo Alto VPN Configuration, and Zone Protection. This creates a broader Enterprise Firewall Training experience while remaining focused on the capabilities defined in EDU-210. Participants therefore gain not only product knowledge, but also a structured understanding of how Palo Alto Networks firewalls support secure and reliable enterprise network operations.