Training Course

Firewall 10.1 Essentials: Configuration and Management (EDU-210)

Duration: 5 Days **Product Version:** PANOS 10.1

Description

The EDU-210 course combines instructor-led training and interactive hands-on labs to build a working knowledge of how to configure and manage Palo Alto Networks® Next-Generation Firewalls. The five days of training will help to:

- Configure and manage the essential features of Palo Alto Networks Next-Generation Firewalls.
- Configure and manage Security and NAT policies to enable approved traffic to and from zones.
- Configure and manage Threat Prevention strategies to block traffic from known and unknown IP addresses, domains, and URLs.
- Monitor network traffic using the interactive web interface and firewall reports.

Target Audience

The course includes hands-on experience configuring, managing, and monitoring a firewall in a lab environment. It is targeted at Security Administrators, Security Engineers, Security Operations Specialists, Security Analysts, and Support Staff.

Anyone planning to attend the Firewall 10.1: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214), Panorama 10.1: Manage Firewalls at Scale (EDU-220), and Firewall 10.1: Troubleshooting (EDU-330), are strongly recommended to complete this course before attending those courses.

Prerequisite Requirements

The following is required when attending the course:

- Basic familiarity with networking concepts including routing, switching and IP addressing
- Familiarity with basic security concepts
- Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

Certification

The EDU-210 course is the recommended training for taking the Palo Alto Networks Certified Network Security Administrator (PCNSA) exam. Additionally, this course combined with the Firewall 10.1: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214) and Panorama 10.1: Manage Multiple Firewalls (EDU-220) courses are the recommended training for anyone planning on taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification exam, or any of the Palo Alto Networks® Systems Engineer certifications.

Course Outline

Day 1

- Palo Alto Networks Portfolio and Architecture
- Configuring Initial Firewall Settings
- Manage Firewall Configurations
- Manage Administrator Accounts

Day 2

- Connecting the Firewall to Production Networks with Security Zones
- Creating and Managing Security Policy Rules
- Creating and Managing NAT Policy Rules

Day 3

- Controlling Application Usage with App-ID
- Blocking Known Threats Using Security Profiles
- Blocking Inappropriate Web Traffic with URL Filtering

Day 4

- Blocking Unknown Threats with Wildfire
- Controlling Access to Network Resources with User-ID
- Using Decryption to Block Threats in Encrypted Traffic

Day 5

- Locating Valuable Information Using Logs and Reports
- What's Next in Your Training and Certification Journey
- Appendices Demos/Capstone Lab

+ Course details are subject to change

Please contact Training@exclusive-networks.com for all onsite training requests, quotes & about partner training requests