Training Course

Firewall 10.1 : Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214)

Duration: 3 Days **Product Version:** PANOS 10.1

Description

The Firewall 10.1 Improving Security Posture and Hardening PAN-OS Firewalls course is three days of instructor-led training that will help you to:

- Determine the efficacy of your current security policies
- Develop workflows for managing your security posture
- Identify rule usage across security policy sets
- Modify your existing policy set to implement Security Best Practices
- Monitor network traffic using the interactive web interface and firewall reports
- Utilize tools such as the BPA tool to further understand your environment

Successful completion of this course will assist in maintaining and managing and existing Palo Alto Networks Firewall protected environment, improve non-greenfield environments, and ensure configurations match security best practice.

Target Audience

This course is intended for Security Administrators, Security Engineers, Security Operations Specialists, Security Analysts, and Support Staff.

Prerequisite Requirements

The following is required when attending the course:

- Complete the Firewall 1010 Essentials: Configuration and Management (EDU-210) or equivalent experience
- Basic familiarity with networking concepts including routing, switching, and IP addressing
- Basic familiarity with networking concepts, including routing, switching, and IP addressing.

Certification

The EDU-214 course is a recommended training for taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) exam. Additionally, the Firewall 10.1 Essentials: Configuration and Management (EDU-210) and Panorama 10.1: Manage Multiple Firewalls (EDU-220) courses are the other recommended training courses for anyone planning on taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification exam.

+ Course details are subject to change

Course Outline

Day 1

- Introduction
- Security Profile Revision
- Daily Operations and Maintenance
- Establish Initial Baseline Visibility.

Day 2

- Analyse and Update Security Rules Passing Traffic
- Inbound Security Rules Best Practices and Analysis
- Outbound Security Rules Best Practices and Analysis

Day 3

- Internal Security Rules Best Practices and Analysis
- Administratively Hardening PAN-OS
- Reducing Policy set and Simplification