

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

Course Summary

Description

Successful completion of this three-day, instructor-led course will help the student manage and maintain a Palo Alto Networks firewall-protected environment. The student will learn how to improve non-greenfield environments and will be better equipped to ensure that configurations match security best practices. The student will also be able to develop an operational strategy for maintaining a high level of compliance.

Objectives

At the end of this course, students will be able 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
- Use the interactive web interface and firewall reports to monitor network traffic
- Use tools such as the BPA tool to further understand your environment

Topics

- Introduction
- Security Profile Revision
- Daily Operations and Maintenance
- Establish Initial Baseline Visibility
- Analyze and Update Security Rules that Pass Traffic
- Inbound Security Rules Best Practices and Analysis
- Outbound Security Rules Best Practices and Analysis
- Internal Security Rules Best Practices and Analysis
- Administratively Hardening PAN-OS
- Reducing Policy Set and Simplification

Audience

Security Engineers, Security Administrators, Security Operations Specialists, Security Analysts, and Support Staff.

Prerequisites

Students must have completed the 'Firewall Essentials: Configuration and Management' course. Students also should be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is an advantage.

Duration

Three days