Palo Alto Networks: Firewall Essentials: Configuration and Management v8.1 (EDU-210)

Duration
5 days

Palo Alto Networks next-generation firewalls are architected to safely enable applications and prevent modern threats. Their approach identifies all network traffic based on applications, users, content and devices, and lets you express your business policies in the form of easy-to-understand security rules.

Flexible deployment options and native integration with their next-generation security platform extend the policy enforcement and cyberthreat prevention to everywhere your users and data are located: in your network, on your endpoints and in the cloud.

Course Overview and Objectives

Successful completion of this five-day, instructor-led course should enhance the student's understanding of how to configure and manage Palo Alto Networks® next-generation firewalls. The student will get hands-on experience configuring, managing, and monitoring a firewall in a lab environment. This training should enable you to:

- Configure and manage the essential features of Palo Alto Networks® next-generation
- firewalls
- Configure and manage GlobalProtect to protect systems that are located outside of the data center perimeter
- Configure and manage firewall high availability
- Monitor network traffic using the interactive web interface and firewall reports

Scope and Target Audience

Scope:

- Course level: Introductory
- Course duration: 5 Days
- Course format: Combines lecture and hands-on labs
- Platform supported: Palo Alto Networks® next-generation enterprise firewalls running the PAN-OS® operating system

Target Audience:

- Security Engineers
- Security Administrators

- Security Operations Specialists
- Security Analysts
- Network Engineers
- Support Staff

Prerequisites

Students must have a basic familiarity with networking concepts including routing, switching, and IP addressing. Students also should be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

Agenda

This class is comprised of the following modules focusing on equipping the student to configure and manage Palo Alto Networks® next-generation firewalls.

- Module 1: Next-Generation Security Platform and Architecture
- Module 2: Virtual and Cloud Deployment
- Module 3: Initial Configuration
- Module 4: Interface Configuration
- Module 5: Security and NAT Policies
- Module 6: App-ID™
- Module 7: Content-ID™
- Module 8: URL Filtering
- Module 9: Decryption
- Module 10: WildFire™
- Module 11: User-ID™
- Module 12: GlobalProtect™
- Module 13: Site-to-Site VPNs
- Module 14: Monitoring and Reporting
- Module 15: Active/Passive High Availability
- Module 16: Next-Generation Security Practices