Firewall 9.0 Essentials: Configuration and Management (EDU-110)

The Palo Alto Networks Firewall 9.0 Essentials: Configuration and Management (EDU-110) course is a self-paced, digital-learning training that describes the essential features that you must address to successfully deploy a Palo Alto Networks Next-Generation Firewall.

This training serves as a preparatory course and as refresher course for the instructor-led Firewall 9.0 Essentials: Configuration and Management (EDU-210) course. You can also use this training to help you to prepare for the PCNSA certification exam.

### Course Modules

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

### Objectives

Successful completion of this self-paced digital-learning training should enhance your understanding of how to configure and manage Palo Alto Networks next-generation firewalls. You should learn how to configure, manage, and monitor a firewall and also have the opportunity to use a lab environment to gain hands-on experience.

### Target Audience


### Prerequisites

Participants 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.

This digital learning training is available at the Learning Center.

### Palo Alto Networks Education

The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks and safely enable applications.