EDU-210
Firewall Essentials: Configuration and Management

Overview

The Palo Alto Networks Firewall Essentials: Configuration and Management (EDU-210) course is five days of instructor-led training that will help you 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.

Course 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 course includes hands-on experience configuring, managing, and monitoring a firewall in a lab environment.

Scope

- Level: Introductory
- Duration: 5 days
- Format: Lecture and hands-on labs
- Platform support: Palo Alto Networks next-generation firewalls running the PAN-OS® operating system version 10.1

Target Audience

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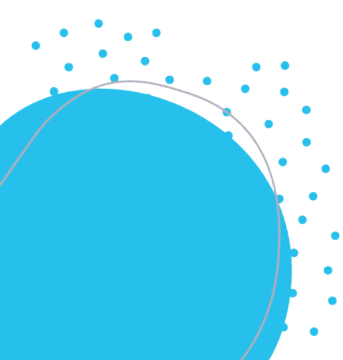
Prerequisites

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.

Course Contents

- Palo Alto Networks Portfolio and Architecture.
- Configuring initial firewall settings.
- Managing firewall configurations.
- Managing firewall administrator accounts.
- Connecting the firewall administrator accounts.
- Connecting the firewall to production networks with security zones.
- Creating and managing security policy rules.
- Creating and managing NAT policy rules.
- Controlling application usage with App-ID.
- Blocking known threats using security profiles.
- Blocking inappropriate web traffic with URL filtering.
- Blocking unknown threats with WildFire.
- Controlling access to network resources with User-ID.
- Using Decryption to block threats in encrypted traffic.
- Locating valuable information using logs and reports.
- What's next in your training and certification journey.
- Appendix A – Securing endpoints with GlobalProtect.
- Appendix B – Providing firewall redundancy with high availability.
- Appendix C – Connecting remotes sites using VPNs.
- Appendix D – Configuring User-ID windows agent.