Firewall Essentials: Configuration and Management

Course EDU-210 5 Days Instructor-led, Hands-on

Introduction

The Palo Alto Networks Firewall 11.0 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

Who Should Attend?

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

At Course Completion

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 should learn and get hands-on experience configuring, managing, and monitoring a firewall in a lab environment.

Outline

Module 1: Palo Alto Networks Portfolio and Architecture

Module 2: Configuring Initial Firewall Settings

Module 3: Managing Firewall Configurations

Module 4: Managing Firewall Administrator Accounts

Module 5: Connecting the Firewall to Production Networks with Security Zones

Module 6: Creating and Managing Security Policy Rules

Module 7: Creating and Managing NAT Policy Rules

Module 8: Controlling Application Usage with App-ID

Module 9: Blocking Known Threats Using Security Profiles

Module 10: Blocking Inappropriate Web Traffic with URL Filtering

Module 11: Blocking Unknown Threats with Wildfire

Module 12: Controlling Access to Network Resources with User-ID

Module 13: Using Decryption to Block Threats in Encrypted Traffic

Module 14: Locating Valuable Information Using Logs and Reports

Module 15: What's Next in Your Training and Certification Journey

- Supplemental Materials
- Securing Endpoints with GlobalProtect
- Providing Firewall Redundancy with High Availability
- Connecting Remotes Sites using VPNs
- Blocking Common Attacks Using Zone Protection