Firewall 11.0 Essentials: Configuration and Management (EDU-210)

Course Description

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

Prerequisites

Students must be familiar 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 Duration:

5 days

Objectives:

Successful completion of this five-day, instructor-led course should enhance the student's understanding of configuring and managing Palo Alto Networks Next-Generation Firewalls. The course includes hands-on experience configuring, managing, and monitoring a firewall in a lab environment.

Course Outline:

1. Palo Alto Networks Portfolio and Architecture
2. Configuring Initial Firewall Settings
3. Managing Firewall Configurations
4. Managing Firewall Administrator Accounts
5. Connecting the Firewall to Production Networks with Security Zones
6. Creating and Managing Security Policy Rules
7. Creating and Managing NAT Policy Rules
8. Controlling Application Usage with App-ID
9. Blocking Known Threats Using Security Profiles
10. Blocking Inappropriate Web Traffic with URL Filtering
11. Blocking Unknown Threats with Wildfire
12. Controlling Access to Network Resources with User-ID
13. Using Decryption to Block Threats in Encrypted Traffic
14. Locating Valuable Information Using Logs and Reports
15. What's Next in Your Training and Certification Journey
16. Supplemental Materials
17. Securing Endpoints with GlobalProtect
18. Providing Firewall Redundancy with High Availability
19. Connecting Remotes Sites using VPNs
20. Blocking Common Attacks Using Zone Protection

Who Should Attend

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