Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

9201 Dry Creek Rd. Centennial, CO 80112, United States

Email: arrow_learning@arrow.com
Phone: 303 790 2330

Firewall 10.2 Essentials: Configuration and Management (EDU-210)

CODE:	LENGTH:	PRICE:
PAN-210	40 Hours (5 days)	$4,995.00

Description

The Palo Alto Networks Firewall 10.0 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

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.

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.

Programme

1. **Palo Alto Networks Portfolio and Architecture**
2. **Connect to the Management Network**
3. **Manage Firewall Configurations**
4. **Manage Firewall Administrator Accounts**
5. **Connect to Production Networks**
6. **The Cyberattack Lifecycle**
7. **Block Threats Using Security and NAT Policies**
8. **Block Packet- and Protocol-Based Attacks**
9. **Block Threats from Known Bad Sources**
10. **Block Threats by Identifying Applications**
11. **Maintain Application-Based Policies**
12. **Block Threats Using Custom Applications**
13. **Block Threats by Identifying Users**
14. **Block Threats by Identifying Devices**
15. **Block Unknown Threats**

16. **Block Threats in Encrypted Traffic**
17. **Prevent Use of Stolen Credentials**
18. **Block Threats Using Security Profiles**
19. **View Threat and Traffic Information**
20. **Next Steps**

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.