FIREWALL: Configuration and Management (EDU-210)

Duration: 5 Days **Course Code: PAN-EDU-210**

Overview:

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 environmenr,

Target Audience:

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

Objectives:

- **After completing this course you should be able to:**
- Configure and manage the essential features of Palo Alto Networks nextgeneration firewalls
- Configure and manage GlobalProtect to protect systems that are located outside of the data center perimeter
- Configure and manage firewall high availability
- Monitor network traffic using the interactive web interface and firewall reports

Prerequisites:

Attendees should meet the following prerequistes:

- 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.

Testing and Certification

Recommended as preparation for the following exam:

- **ACE** - Accredited Configuration Engineer Exam
- **PCNSE** - Palo Alto Networks Certified Network Security Engineer

Follow-on-Courses:

The following courses are recommended for further study :

- **PAN-EDU-221** - Panorama 9.0: Manage Multiple Firewalls (EDU-221)

Content:

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 Life cycle
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

Further Information:

For More information, or to book your course, please Email us on:

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

UAE - training.emea@clclearningafrica.com