Palo Alto Network Security Engineer

Course Duration- 10 Days 80 Hours

Objectives

Successful completion of this 10-day, instructor-led course should

enhance the student's understanding of configuring and managing

Palo Alto Networks Next-Generation Firewalls. Managing Firewall at Scale, and Troubleshooting.

Learn how to configure and manage the next-generation Panorama management server

- Gain experience configuring templates (including template variables) and device groups
- Gain experience with administration, log collection, and logging and reporting
- Become familiar with planning and design considerations for Panorama deployment
- Participants will perform hands-on troubleshooting related to the configuration and
- operation of the Palo Alto Networks firewall.

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

Target Audience

- Security Engineers
- Security Administrators
- Security Operations Specialists
- Security Analysts
- Support Staff

Prerequisites

- Participants must be familiar with networking concepts, including

  routing, switching, and IP addressing.

- Participants also should be familiar with basic security concepts.
- Experience with other security technologies (IPS, proxy, and

  content filtering) is a plus.

Course Modules

First Part 5 Days

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-Blocking Common Attacks Using Zone Protection

Supplemental Materials

Securing Endpoints with GlobalProtect

Providing Firewall Redundancy with High Availability

Connecting Remotes Sites using VPNs

SECOND PART

Panorama

2 Days

Course Modules

1 - Initial Configuration

2 - Adding Firewalls

3 - Templates

4 - Device Groups

5 - Log Collection and Forwarding

6 - Using Panorama Logs

7 - Panorama Administrative Accounts

8 - Reporting

9 – Troubleshooting

THIRD PART

Palo Alto Firewall: Troubleshooting

3 Days

Course Modules

1 - Tools and Resources

2 - Flow Logic

3 - Packet Captures

4 - Packet-Diagnostics Logs

5 - Host-Inbound Traffic

6 - Transit Traffic

7 - System Services

8 - Certificate Management and SSL

Decryption

9 - User-ID

10 - GlobalProtect

11 - Support Escalation and RMAs