Palo Alto Firewall Expert Course Overview

Palo Alto Firewall is the next generation firewall which has been deployed in data centers and branch offices across many fortunate 500 companies.

About the Training

This course is specially designed to provide a solid foundation from basic to advance level for network security professionals to enhance their next-generation firewall skills. This course will provide you hands-on exposure to install, configure, manage and troubleshoot Palo Alto firewall in a production environment.

Online –Weekend Classes

- **Study Material: -** Instructor-led live training, live training Streaming Recorded Videos, Online Lab Workbook, andRemote Virtual Lab access.
- **Duration:-** 1 Month

Certification:

It will also help them to prepare the Palo Alto Certified Network Security Engineer (PCNSE) certification exam.

Requirements

Interested candidates should have basic concepts of basic level networks and security with IP addressing, TCP/IP, OSI layers and packet flows skills and knowledge.

Working experience in firewalls would be an advantage for interested candidates.

Target Audience

- Network security specialist
- Network security professionals
- Network security analyst
- Network specialist
- Network security consultants

What you will learn:

- Introduction lecture and hands-on training for Palo Alto Firewall hardware concepts
- You will learn vulnerability protection security profiles
- Antispyware security profile
- Antivirus security profiles
- Packet Filtering
- Zone protection
- Virtual system benefits
- How to implement site-to-site VPN
- NAT policies
- Detail concepts about SSL, encryption, and decryption
- Details about APP ID overview
- Network security management

About Instructor

The Palo Alto course you are going to learn from highly experienced and industry expert. Trainer is working professional and have working experience with Palo Alto firewalls. He has over 10 years working industry experience.

Course Content

Module 1: Platforms and Architecture

- Single Pass Architecture
- Flow Logic

Module 2: Initial Configuration

- Initial Access to the System
- Configuration Management
- Licensing and Software Updates
- Account Administration

Module 3: Interface Configuration

- Security Zones
- Layer 2, Layer 3, Virtual Wire, and Tap
- Sub-interfaces
- DHCP

- Virtual Routers

Module 4: Security and NAT Policies

- Security Policy Configuration
- Policy Administration
- NAT (source and destination)

Module 5: App-ID

- App-ID Overview
- Application Groups and Filters

Module 6: Content-ID

- Antivirus
- Anti-spyware
- Vulnerability
- URL Filtering

Module 7: File Blocking: Wildfire

- Security Profiles File Blocking
- Wildfire

Module 8: Decryption

- Certificate Management
- Outbound SSL Decryption
- Inbound SSL Decryption

Module 9: User-ID

- Enumerating Users
- Mapping Users to IP addresses
- User-ID Agent

Module 10: Site-to-Site VPN

- IPsec Tunnels

Module 11: Management & Reporting

- Dashboard
- Basic Logging
- Basic Reports
- Panorama

Module 12: Active/Passive High Availability

- Configuring Active/Passive HA

Note: ***Most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You
Visit us
https://www.uninets.com/