Palo Alto

Prerequisites:

Students must have a basic familiarity with networking concepts including routing, switching, and IP addressing. Students should also be familiar with basic port-based security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

Mod 1: Platforms and Architecture

- Single-Pass Architecture
- Flow Logic

Mod 2: Initial Configuration

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

Mod 3: Basic Interface Configuration

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

Mod 4: Security and NAT Policies

- Security Policy Configuration
- Policy Administration
- NAT (source and destination)
- U-NAT for LAN
- U-NAT for DMZ

Mod 5: Basic App-ID

- App-ID Overview
- Application Groups and Filters
- Custom Applications.
- Application Override

Mod 6: Basic Content-ID

- Antivirus
- Ant-spyware
- Vulnerability
- URL Filtering
- Data Filtering
- DoS Protection
- Custom Threat Signatures

Mod 7: File Blocking and WildFire

- File Blocking
- WildFire

Mod 8: Decryption

- Certificate Management
- Outbound SSL Decryption
- Inbound SSL Decryption

Mod 9: Basic User-ID

- Captive Portal
- LDAP Integration
- Enumerating Users
- Mapping Users to IP Addresses
- User-ID Agent
- Terminal Server Agent
- XML API

Mod 10: VPNs

- IPSec Tunnels
- Implementation of Global Protect

Mod 11: Management and Reporting

- Dashboard
- Basic Logging
- Basic Reports
- Panorama

Mod 12: High Availability

- Configuring Active/Passive HA
- Configuring Active/Active HA

Mod 13: Migration

- CISCO ASA to PaloAlto

Mod 14: T-shoot

CLI

Mod 15: PaloAlto Cloud Deployment