PALO ALTO NETWORKS - Course Content

- **Introduction to Palo Alto Networks**
  - About Palo Alto Networks.
    Single Pass & Parallel processing.
    Control Plane & Data Plane.
- **Security Terminologies**
  - Understanding Assets, Vulnerabilities, Exploit, Threats, Attacks & Countermeasures.
  - Malware- Virus, Adware, Ransom ware, Trojan, Worm, Spyware, Rootkits, Key logger.
  - Goal of Security CIA – Confidentiality, Integrity, Availability.
- **Setting up Palo Alto Lab**
  - Download & importing to VMware Workstation Professional.
  - Adding required Nodes & Accessing device, Login into Firewall.
- **CLI Access Modes & Dashboard Tabs**
  - Modes of Palo Alto – Operational Mode, Configuration Mode.
  - CLI Management Commands, Functional category tabs, widgets etc.
- **Licenses, Updates & DNS NTP Configurations**
  - Activate Licenses – Threat prevention, URL Filtering, Wildfire, Global Protect etc.
  - Dynamic updates & Software Updates.
  - Configuring DNS, NTP settings.
- **Zones & Interfaces Configuration**
  - Zone Types- INSIDE, OUTSIDE & DMZ
  - Interface Types -TAP, LAYER2, LAYER3, VIRUTAL WIRE, HA
  - Configuring Zones & Interfaces, verifying reachability
- **Virtual Router**
  - Configuring static, default routing
  - Configuring RIP & OSPF
  - Configuring Redistribution between RIP & OSPF

- **Security Policies Concepts**
  - Components of security polices Rules.
  - Security policy actions
  - Create a security policy Rule.
- **Network Address Translation**
  - NAT Policy Rules
  - Source NAT & Destination NAT
  - Types source NAT-Dynamic ip & port, Static and Dynamic
  - Configuring source NAT & Destination NAT
- **Security Profiles & Security Groups**
  - URL filtering profile
  - Vulnerability protection profile
  - File blocking profile
  - Wildfire analysis profile
  - Data filtering profile
  - Creation of security profile groups
- **APP-ID Overview**
  - Identifying the application- application signature, unknown protocol decoder, known protocol decoder, protocol decryption.
  - Application shifts-TCP 3 way-handshake, Web-browsing, SSL, base
  - Dependencies, Vulnerabilities & Implicitly use of the applications
  - Using APP-ID in the polices
  - Customizing and Application Override
- **User-ID & LDAP Integration**
  - Integration of LDAP authentication server with Palo Alto
  - Security policies based on users & verification of logs.

- **Deployment Methods of Palo Alto**
  - Layer2 deployment- Creating Vlan, adding interfaces, monitor logs.
  - Tap mode deployment- Configure Layer3 switch a span port, monitor logs.
  - Virtual wire deployment- Configuring Palo Alto as bump in wire.
  - SSL forward proxy- Using self-signed certificate for decryption.
- **DHCP & DHCP Relay Agent**
  - DHCP overview, firewall as DHCP server and Client
  - DHCP Messages, Addressing, Options
  - Configuring an interface as a DHCP Server
  - Configuring an interface as a DHCP Relay Agent
- **Syslog Server & Net flow server for Monitoring Palo Alto**
  - Syslog server Field Descriptions
  - Configuring Syslog server for Monitoring
  - Configuring net flow exports
- **VPN concept, site to site, remote user-to-site**
  - Configuring site to site vpn & Analysing ESP encrypted traffic
  - Configuring Global protect portals, gateways, connects sites using Global Protect application.