PALO ALTO NETWORK SECURITY TRAINING

UPGRADE YOUR KNOWLEDGE

Palo Alto Network Security Training

Course Overview

Palo Alto certification validates your ability to configure the central features of Palo Alto Networks Next Generation Firewall and capability to effectively deploy the firewalls to enable network traffic based on who (User-ID), what (App-ID), and when (Policy), all while ensuring security (Content-ID). Demonstrate your ability to configure the central features of Palo Alto Networks Next Generation Firewall and capability to effectively deploy the firewalls to enable network security.

Duration & Module Coverage

Duration: 13 Days (32hrs)

Session Options	Module Coverage
Session Weekdays: 2.5 hours per day. 4 days per week. **Session Weekends:** 2.5 hours per day.	**Day 1** - **Modules 1 to 2** **Day 2** - **Module 3** **Day 3** - **Module 4** **Day 4** - **Module 5 to 6** **Day 5** - **Module 7 to 9** **Day 6** – **Module 10** **Day 7** – **Module 11** **Day 8** – **Module 12** **Day 9 – Module12 [contd.]** **Day 10 – Module13** **Day 11 – Module 14** **Day 12 – Module 15** **Day 13 – Module 16**

Learning Goals

By the end of this course participants will be able to:

1. Demonstrate knowledge of the Palo Alto PANOS devices.
2. Understand security technologies used in Palo Alto Firewalls.
3. Configuration and troubleshooting skills of related platforms.

Pre-Requisites

This course is for security professionals looking to work in a Palo Alto environment. Knowledge of basic networking including OSI and TCP/IP Model and sub-netting is mandatory to attend this course.

Teaching Methodology

This is a very hands-on course where participants carry out practical exercises according to the lab guide provided. The concepts are taught through implementation of real-world use-cases. Our exercises have been carefully designed to replicate scenarios participants will face in real life work conditions.

Who Should Take This Course?

This course is designed for security professionals with knowledge of basic networking looking forward to gain understanding of security technologies offered by Palo Alto Next-Generation Firewalls and configuration and troubleshooting of related platforms.

Course Content

1. **Platform and Architecture**
   - Understand meaning of next generation firewall [NGFW].
   - Introduction to different firewalls models in the market and market ranking of Palo Alto.
   - Parameters for deciding firewall for a network
   - Stateless vs Stateful Firewalls
   - Architecture of Palo-Alto OS and firewall platforms covering VM firewalls and hardware firewalls.
   - Application of various platforms suiting to different network environments

2. **Initial Configuration of Firewall**
   - Introduction to WebUI and CLI of Palo Alto.
   - Default setting on Palo Alto firewalls.
   - Configuration of initial parameters- DNS setting, passwords, login IP.
   - Saving and loading configurations.
   - Types of admin accounts and creating multiple admins.
   - Locks available in WebUI.
   - Setting up passwords and password complexities.
   - Updating Signature Database and Licensing of Firewall
   - Setting up of the basic network.

3. **Interface Configuration**
   - Types of interfaces available in firewall- Layer 3, Layer 2, HA, Tap and Virtual-Wire.
   - Choosing type of interface for particular network design.
   - Configuring interfaces depending on network design.
   - Configuring Virtual-Wire, VLANs and Virtual Router.
   - Routing in Palo Alto- Static, OSPF, BGP.
   - Setting up service route on firewall.
   - Configuring parameters on management interface via CLI and WebUI.

4. **Security and NAT Policies**
   - Types of security policies.
   - Configuration and logical design of policies.
   - Order of processing the policies by the firewall.
   - Enabling and disabling policies.
   - External Dynamic Lists [EDL] and usage in security policies.
   - Pre-defined and user-defined EDL.
   - Uses of profiles in policies.
   - Actions in security policies- Allow, Drop, Deny, Reset Server, Reset Client, Reset both.
   - Understanding and configuration of types of NAT- static, dynamic, PAT, source and destination.

5. App-ID

- Understand TCP packets and how NGFW firewalls process them.
- Drawbacks faced by traditional firewalls in understanding Layer-7 applications.
- Application detection mechanism in Palo Alto
- Applipedia, Implicit and explicit application dependencies
- Application groups and Application fitlers.
- Configure App-ID, Application Exceptions, Custom Apps and Application override policy.

6. Content-ID

- Content inspection using SP3 architecture.
- Security profiles- Anti-virus, Anti-Spyware, Vulnerability, File Detection and Data filtering
- Applying security profile in security policies.
- DNS Sinkholing in Palo Alto.
- Exceptions handling in profiles.
- Configure Content-ID in PAN-OS.

7. URL Filtering

- URL categorization.
- Updating URL Database.
- Actions taken in URL filtering policy.
- Credential phishing avoidance policy in Palo Alto.
- Configuration of URL filtering.
- Setting override password in Palo Alto.

8. SSL Decryption

- Working of SSL to establish encrypted session.
- Why SSL decryption is needed?
- Types of SSL Decryption- SSL Forward Proxy, SSL Inbound Inspection and SSH Proxy
- Self-signed certificate versus CA signed certificate.
- Configure PAN-OS where to do and where to avoid SSL decryption.
- Enable SSL Opt-out Page for users.
- Verify SSL Decryption in traffic logs.

9. Working of Wildfire

- What is wildfire?
- Why is Wildfire so important in modern day networks?
- Configure wildfire in Palo Alto Network firewall.
- Wildfire analysis in public cloud and private cloud.
- Widlfire licensing and subscriptions
- Understanding of wildfire reports.

10. GlobalProtect VPN

- What is GlobalProtect VPN?
- Configure GlobalProtect Portal and Gateway.
- Use GlobalProtect App for Windows, Linux and iOS

11. Site-to-Site IPSec VPNs

- Understanding of IPSec site to site VPNs.
- Understand IPSec Phase-1 and Phase-2 profiles.
- Difference between Main mode and aggressive mode in phase-1 and usecases.
- How does Diffie-Helman Exchange works.
- Features offered by Palo Alto to secure IPSec VPNs fromintruders.
- Configuration of IPSec VPN between two firewalls.
- Considerations when deploying VPN with third party vendordevice.
- Monitoring an IPSec VPN.

12. User-ID

- Overview of User-ID
- User-ID Concepts
- Types of user mapping- server monitoring, port mapping, XFF headers, syslog,GlobalProtect, XML API.
- Configure Captive Portal in Palo Alto Networks Firewall
- Service account for user-ID agents.
- Map IP addresses to users.
- Deploy user-ID in a large scale network.
- Verify user-ID configuration

13. Monitoring Reports in Palo Alto

- Monitor threat logs in Palo Alto
- Take packet captures
- Generate reports for logs
- Generate customized reports
- Schedule PDF reports over email.
- Use Application Command Center.

14. Active/Passive High Availability

- High Availability Overview.
- High Availability Concepts in Palo Alto.
- Setup Active/Passive HA.
- Selection of Active firewall.
- High Availability Synchronization.
- High Availability Firewall States.
- Design layout for Active/Passive and Active/Active HA.
- Monitor and troubleshoot High Availability.

15. Quality of Service

- QoS for application and users.
- QoS policy.
- QoS profiles and classes.
- QoS priority queuing.
- QoS bandwidth management.
- QoS interface mapping.
- Configure and verify QoS policy.

16. Panorama

- Configure management Panorama server.
- Configure template and template variables.
- Configure device groups.
- Install updates for Panorama.
- Modes of operation of Panorama.

Practical Learning Exercises

A lab guide will be provided to each student with requirement scenarios. Along with lab guide required VMs and cloud access will be provided to set up and practice individual labs for self practice.

A sample scenario would consist of one interface of Palo Alto appliance connected to internal network, one interface connected to Server farm and one interface connected to the internet.

Similarly there would be scenarios for implementing, verifying and troubleshooting all modules covered in the course.