Firewall Installation, Configuration, and Management: Essentials I

OVERVIEW

Successful completion of this three-day, instructor-led course will enable the student to install, configure, and manage the entire line of Palo Alto Networks® Next-Generation firewalls.

COURSE OBJECTIVES

Students attending this introductory-level class will gain an in-depth knowledge of how to install, configure, and manage their firewall, as well as configuration steps for the security, networking, threat prevention, logging, and reporting features of the Palo Alto Networks Operating System.

SCOPE

- Course level: Introductory
- Course duration: 3 Days
- Course format: Combines lecture with hands-on labs
- Platform supported: All Palo Alto Networks next-generation firewall models

TARGET AUDIENCE

Security Engineers, Network Engineers, and Support staff

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.

Day 1

Module 1: Platforms and Architecture

- Single Pass Architecture
- Flow Logic

Module 2: Initial Configuration

- Single Pass Architecture
- Flow Logic
- Initial Access to the System
- Configuration Management
- Licensing and Software Updates n Account Administration

Module 3: Interface Configuration

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

Module 4: Security and NAT Policies

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

Day 2

Module 5: App-IDTM

- App-ID Overview

- Application Groups and Filters

Module 6: Content-IDTM

- Antivirus
- Anti-spyware
- Vulnerability
- URL Filtering
- File Blocking: WildFireTM

Module 7: Decryption

- Certificate Management
- Outbound SSL Decryption
- Inbound SSL Decryption

Day 3

Module 8: User-IDTM

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

Module 9: Site-to-Site VPN

- IPsec Tunnels

Module 10: Management & Reporting

- Dashboard
- Basic Logging
- Basic Reports

Module 11: Active/Passive High Availability

- Configuring Active/Passive HA

Module 12: Panorama

- Centralized Configuration and Deployment
- Centralized Logging and Reporting
- Role-Based Access Control

- **ORDERING INFORMATION:**

- **PART NUMBER: PAN-EDU-201**

Firewall Installation, Configuration, and Management: Essentials II

OVERVIEW

Extended Firewall Management is the next-level follow-on course to Palo Alto Networks® Installation, Configuration, and Management (PAN-EDU-201). Extended Firewall Management expands on 201 course topics, while introducing many new features and functions of Palo Alto Networks Next-Generation firewalls.

COURSE OBJECTIVES

Successful completion of this two-day, instructor-led course will enhance the student's understanding of how to install, configure, manage, and perform basic troubleshooting on the entire line of Palo Alto Networks Next-Generation firewalls.
Additionally, students will be instructed on the basics of implementing and managing GlobalProtect and Active/Active High Availability. Students will gain an in-depth knowledge of how to optimize their visibility and control over applications, users, and content.

SCOPE

- Course level: Introductory
- Course duration: 2 Days
- Course format: Combines Instructor-led and hands-on labs
- Platform support: All Palo Alto Networks next-generation firewall models running PAN-OS.

TARGET AUDIENCE

Security Engineers, Network Engineers, and Support staff

PREREQUISITES:

Completion of Firewall Installation, Configuration, and Management (201) or equivalent experience is highly recommended.
Students must have a basic familiarity with networking concepts including routing, switching, IP addressing, and basic port-based security concepts.

Day 1

Module 1: Advanced Interface Config

- Advanced NAT
- Policy Based Forwarding
- Routing Protocols (OSPF)

Module 2: App-IDTM: Custom Apps

- Defining new Application Signatures
- Application Override

Module 3: Advanced Content-IDTM

- Custom Threat Signatures

- Data Filtering
- DoS Protection
- Botnet Report

Module 4: Advanced User-IDTM

- Terminal Server Agent
- Captive Portal
- XML API

Day 2

Module 5: QoS

- Configuring Quality of Service

Module 6: Monitoring and Reporting

- Log Forwarding
- SNMP
- Vulnerability
- Reporting

Module 7: GlobalProtect

- Implementation of GlobalProtect
- Install and Configure Portal, Gateway, and Agents

Module 8: MSM

- GP-100 Overview
- Deployment Policies
- Managing Mobile Devices

Module 9: Active/Active High Availability

- Configuring Active/Active HA