FireWall Security Best Practices and Threat Prevention (EDU-214)

Course Description

The Palo Alto Networks **"FireWall Security Best Practices and Threat Prevention"** (EDU-214 replacement) course is an instructor-led training that will help you to:

- Determine the efficacy of your current security policies
- Develop workflows for managing your security posture
- Modify your existing policy set to implement Security Best Practices
- Monitor network traffic using the interactive web interface and firewall reports
- Utilize tools such as the BPA tool to understand your environment further

This course enables you to effectively secure your enterprise network by leveraging the full potential of the Next-Generation FireWall. Most firewall infrastructures have been migrated from a legacy firewall. However, such a like-for-like migration does not protect the network as it is missing the correct setup of all the threat prevention techniques offered by the Next-Generation FireWall. Implementing security best practices can be a serious challenge as it is often difficult to identify where to start and what combination of best practices is adequate for the environment. Therefore, the "FireWall Security Best Practices and Threat Prevention" (EDU-214 replacement) course teaches not only security best practices but also the methodologies to apply them with minimal impact effectively. Please see the course content for the detailed agenda.

Prerequisites

The "Firewall Configuration and Management" (EDU-210) course or equivalent practical experience working with the Palo Alto Networks Next-Generation FireWall is a recommended prerequisite to taking this optimizing firewall threat prevention PAN EDU 214 course. Students also should be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is an advantage.

Course Duration:

3 days

Course Outline:

Introduction

- Course overview
- Course scenario description
- BPA tool, ACC, logging, and reporting
- Lab architecture

Security Profiles

- Review of Content-ID
- Defining context for Security Profiles
- Creation of profile groups

Daily Operations and Maintenance

- Software release cycle
- App-ID and threat update best practices and process
- Policy description and audit best practices

Establish Initial Baseline Visibility

- Log Forwarding Profiles
- Syslog, email, SNMP traps, and formatting
- Custom and pre-made reporting
- Dynamic user and address groups

Analyze and Update Security Rules Passing Traffic

- Expedition for BPA
- Policy Optimizer
- Application-centric rules
- Categorizing traffic into Inbound, Outbound, and Internal flows

Inbound Security Rules Best Practices and Analysis

- Inbound threat protection
- Workflow for false positives
- Inbound SSL Decryption best practices

Outbound Security Rules Best Practices and Analysis

- User-ID
- URL Filtering Profiles
- Credential theft
- Custom URL categories
- Outbound SSL decryption best practices

Internal Security Rules Best Practices and Analysis

- Internal traffic security best practices
- Internal traffic requirement workflows
- Application Override policies
- Intrazone traffic best practices

Administratively Hardening PAN-OS

- Role-based access control
- Multi-factor authentication
- Administrative best practice principles
- Hardening administrative interfaces

Reducing Policy set and Simplification

- Tag unused rules using Policy Optimizer
- Implement policy hygiene
- Describe how to use Address Groups and regions to reduce the policy set
- Describe Zero Trust architecture

Who Should Attend

- Security Engineers
- Security Administrators
- Security Operations Specialists
- Security Analysts
- Support Staff