

# PA-FND (PALO-ALTO FOUNDATIONS) 1.0

## Objetivo

Podemos destacar os principais objetivos desse treinamento: - Compreensão do Portfólio e Arquitetura da Palo Alto Networks - Como Proceder as Configurações Iniciais (CLI & GUI) - Compreender a Arquitetura das Configurações da Solução NGFW - Gerenciando O Acesso Administrativo ao Equipamento - Conectando o Firewall em Redes de Produção em Camada 3 - Configurando e Gerenciando as Regras da Política de Segurança - Configurando e Gerenciando Regras da Política NAT - Controlando a Utilização de Aplicativos via Palo Alto App-ID - Como Bloquear Ameaças Utilizando Perfis de Segurança - Como Bloquear Tráfego Web Inapropriado via Filtragem de URL - Compreender a Solução Palo Alto Wildfire - Controlar Acessos aos Recursos da Rede via Palo Alto User-ID - Como Inspeccionar e Bloquear Ameaças no Tráfego Criptografado - Como Implantar Soluções de Acesso Seguro via VPN - Monitorando Informações Utilizando Logs e Relatórios

## Público Alvo

Engenheiros de segurança, Administradores de segurança, Especialistas em operações, analistas de segurança e equipe de suporte.

## Pré-Requisitos

Os alunos devem estar familiarizados com os conceitos de rede, incluindo roteamento, comutação e endereçamento IP. Alunos também deve estar familiarizado com os conceitos básicos de segurança. Desejável experiência com outras tecnologias de segurança (IPS, proxy e filtragem de conteúdo).

## Carga Horária

40 horas (5 dias).

## Conteúdo Programático

- Introdução ao Treinamentos
- Apresentação do Laboratório
- Portfólio e Arquitetura da Palo Alto Networks
- Definindo as configurações iniciais do firewall
- Gerenciando Configurações de Firewall
- Gerenciando contas de administrador de firewall
- Conectando o Firewall a Redes de Produção com as Zonas de segurança
- Criando e Gerenciando Regras de Política de Segurança
- Criando e Gerenciando Regras de Política NAT
- Controlando o uso do aplicativo com App-ID
- Bloqueando ameaças conhecidas usando perfis de segurança
- Bloqueando Tráfego Web Inapropriado com Filtragem de URL

Bloqueando ameaças desconhecidas com Wildfire  
Controle de Acesso aos Recursos de Rede com User-ID  
Usando a Descritografia para Bloquear Ameaças no Tráfego Criptografado  
Localizando informações valiosas usando logs e relatórios

### **Atividades Práticas**

Lab 1: Palo Alto Networks Portfolio and Architecture  
Lab 2: Configuring Initial Firewall Settings  
Lab 3: Managing Firewall Configurations  
Lab 4: Managing Firewall Administrator Accounts  
Lab 5: Connecting the Firewall to Production Networks with Security Zones  
Lab 6: Creating and Managing Security Policy Rules  
Lab 7: Creating and Managing NAT Policy Rules  
Lab 8: Controlling Application Usage with App-ID  
Lab 9: Blocking Known Threats Using Security Profiles  
Lab 10: Blocking Inappropriate Web Traffic with URL Filtering  
Lab 11: Blocking Unknown Threats with WildFire  
Lab 12: Controlling Access to Network Resources with User-ID  
Lab 13: Using Decryption to Block Threats in Encrypted Traffic  
Lab 14: Locating Valuable Information Using Logs and Reports  
Lab 15: Capstone  
Lab 16 (Optional): Site-to-Site VPN  
Lab 17 (Optional): Active/Passive High Availability  
Lab 18 (Optional): GlobalProtect