

Programa de Formação em Gestão de Firewalls com pfSense

1. Nome da Instituição Formadora

Mechanical Tecnologia

2. Objectivos

Este programa tem como objetivo capacitar os participantes com as habilidades necessárias para administrar, configurar e otimizar firewalls e roteadores baseados na plataforma pfSense. O pfSense é uma distribuição de software de código aberto baseada no FreeBSD, amplamente utilizada para proteger redes e fornecer serviços avançados de roteamento e segurança.

3. Publico Alvo

Este programa destina-se Profissionais de TI que desejam aprender a configurar e gerenciar firewalls pfSense, administradores de rede que buscam aprimorar suas habilidades em segurança de rede e estudantes de tecnologia da informação e áreas relacionadas que se interessam por firewalls e segurança de rede.

4. Pré-requisitos

Não são necessários conhecimentos prévios em pfSense ou FreeBSD, porém é recomendável que os participantes tenham familiaridade básica com redes de computadores e administração de sistemas.

5. Metodologia de Ensino

O programa será ministrado através de aulas teóricas e práticas, combinando explicações teóricas, demonstrações ao vivo e exercícios práticos. Os participantes terão a oportunidade de configurar seus próprios ambientes pfSense em laboratório virtual, aplicando os conhecimentos adquiridos em situações reais.

6. Plano Programático

Tópico 1: Introdução ao pfSense

- Introdução ao pfSense: história, características e benefícios.
- Instalação e configuração inicial do pfSense.
- Conceitos básicos de firewall e roteamento.

Tópico 2: Configuração Avançada do pfSense

- Configuração de interfaces de rede: LAN, WAN, DMZ.
- Regras de firewall: filtragem de tráfego, NAT, redirecionamento de portas.
- Configuração de VPN: OpenVPN, IPsec.

Tópico 3: Recursos Avançados do pfSense

- Balanceamento de carga: configuração de load balancing e failover.
- Monitoramento de tráfego: uso de ferramentas de análise de tráfego e logs.
- Filtragem de conteúdo: configuração de proxies e bloqueio de URLs.

Tópico 4: Segurança e Manutenção do pfSense

- Práticas recomendadas de segurança cibernética: atualizações de software, senhas fortes, firewall rulesets.
- Resolução de problemas comuns: diagnóstico de problemas de conectividade, análise de logs.
- Backup e restauração de configurações do pfSense.

Tópico 5: Monitoramento e Solução de Problemas

- Monitorando o desempenho da firewall e identificando problemas de rede.
- Solucionando problemas de conectividade, firewall e VPN.
- Registando eventos de segurança e realizando análises de logs.

7. Aptidões ao fim do curso

Ao final da formação, os participantes serão capazes de:

- Instalar e configurar o pfSense em diferentes ambientes;
- Gerenciar usuários e autenticação;
- Implementar soluções de segurança avançadas;
- Monitorar e solucionar problemas.

8. Carga Horaria

- o 48 Horas