

PROGRAMME DE FORMATION

pfSense et OPNsense : déployer un pare-feu open source

Installer, configurer et maintenir une appliance pare-feu open source sécurisant plusieurs zones et accès distants.

DUREE	NIVEAU	FORMAT	ORGANISATION
3 jours / 21 heures	Intermédiaire	Présentiel ou à distance	Intra-entreprise

Finalité de la formation

Installer, configurer et maintenir une appliance pare-feu open source sécurisant plusieurs zones et accès distants.

Public concerné : Administrateurs systèmes et réseau, techniciens infrastructure et responsables sécurité

Prérequis : Maîtriser TCP/IP, l'adressage, le routage et les principes de filtrage réseau.

Objectifs opérationnels

- Installer une appliance virtuelle et préparer ses interfaces.
- Construire des règles de filtrage lisibles et testables.
- Mettre en oeuvre NAT, VLAN, DHCP et DNS.
- Déployer un VPN utilisateur ou inter-sites.
- Sauvegarder, superviser et dépanner la plateforme.

Programme détaillé

La formation alterne apports ciblés, démonstrations, manipulations guidées et mises en situation adaptées à l'environnement des participants.

SEQUENCE	CONTENUS ET MISES EN PRATIQUE
Jour 1 - Installation et politiques	Architecture et interfaces ; installation ; alias ; règles ; journalisation et tests.
Jour 2 - Services et VPN	NAT ; VLAN ; DHCP et DNS ; VPN IPsec ou WireGuard ; authentification.
Jour 3 - Exploitation et sécurité	Haute disponibilité ; sauvegarde et mise à jour ; supervision ; diagnostic et durcissement.

Atelier ou projet de synthèse

Sécuriser un réseau multi-zones avec accès distant VPN et règles documentées.

Méthodes et évaluation

Démonstrations commentées, travaux pratiques individuels ou en binôme, supports numériques et correction collective. Évaluation par positionnement initial, exercices guidés, mise en situation finale et bilan des acquis.

Accessibilité : le programme et les modalités peuvent être adaptés après analyse des besoins et des contraintes d'accessibilité.