

Objectifs

- ❖ Comprendre l'interface et les avantages d'OPNsense
- ❖ Installer OPNsense sur diverses plateformes et configurer les ressources
- ❖ Créer et gérer les règles de firewall pour sécuriser le réseau
- ❖ Configurer et sécuriser le NAT et les VLAN
- ❖ Configurer des VPN et assurer leur maintenance et optimisation

Public visé

- Administrateurs réseau
- Responsables de la sécurité Pré-requis
- Connaissances de base en réseaux (IP, VLAN, routage)
- Compréhension des principes de la sécurité informatique
 - Expérience avec des systèmes d'exploitation de type Unix/Linux (optionnel, mais recommandé)
- Familiarité avec les concepts de VPN, NAT et firewall

Méthodes pédagogiques Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences. Sanction Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Durée de la Formation :3 Jours (21 heures)

Prix de la Formation :3400 euros TTC

PROGRAMME DE NOTRE FORMATION OPNsense

INTRODUCTION À OPNSENSE

- Présentation d'OPNsense et de son interface
- Avantages d'OPNsense par rapport à d'autres solutions de firewall
- Architecture typique et composants clés
- Scénarios d'utilisation courants
- Tour d'horizon des modules complémentaires disponibles

INSTALLATION ET DIMENSIONNEMENT

- Exigences matérielles et recommandations
 - Installation d'OPNsense sur différentes plateformes (physique, virtuelle)
 - Post-installation : configuration initiale et accès
 - Dimensionnement des ressources en fonction des besoins de sécurité
 - Mise en place d'une stratégie de sauvegarde initiale
- GESTION DES RÈGLES DE FIREWALL**

- Comprendre l'ordre des traitements effectués par OPNsense
- Création et gestion des règles de base du filtrage
- Utilisation des alias pour simplifier la gestion des règles
- Mise en place de règles avancées et de groupes de règles
- Bonnes pratiques et sécurisation du firewall

GESTION DES RÈGLES DE FIREWALL

- Comprendre l'ordre des traitements effectués par OPNsense
 - Création et gestion des règles de base du filtrage
 - Utilisation des alias pour simplifier la gestion des règles
 - Mise en place de règles avancées et de groupes de règles
 - Bonnes pratiques et sécurisation du firewall
- CONFIGURATION DU NAT ET DES VLAN**
- Configuration de base et avancée du NAT (Network Address Translation)
 - Gestion des mappings et des règles de NAT
 - Création et gestion des VLAN (Virtual Local Area Network)
 - Sécurisation et isolation du trafic avec les VLAN
 - Résolution des problèmes courants de NAT et VLAN

PRIORISATION DE TRAFIC ET LIMITERS

- Introduction à la Quality of Service (QoS)
- Configuration des classes de trafic et des politiques de QoS
- Mise en place des limiters pour gérer la bande passante
- Surveillance et ajustement de la performance réseau
- Cas pratiques et simulations

CONFIGURATION DES VPN

- Présentation des types de VPN supportés par OPNsense (IPsec, OpenVPN, etc.)
- Configuration étape par étape d'un VPN
- Gestion des certificats pour sécuriser les VPN
- Bonnes pratiques pour l'exploitation et la maintenance des VPN
- Dépannage et optimisation des performances

VPN GESTION DES UTILISATEURS ET AUTHENTIFICATION

- Configuration des utilisateurs locaux et droits d'administration
- Intégration avec des systèmes d'authentification externes (LDAP, Active Directory)
- Mise en place de politiques de sécurité pour l'accès utilisateur
- Surveillance et audit des activités utilisateurs
- Sécurité renforcée par la gestion des rôles

MISES À JOUR ET MAINTENANCE

- Gestion des mises à jour du système OPNsense
- Planification et application des patches de sécurité
- Mise en place de routines de sauvegarde et de restauration
- Surveillance de l'intégrité du système et des performances
- Stratégies de récupération après incident