+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 18/09/2024

S'inscrire

Formation OPNsense

3 jours (21 heures)

Présentation

LUn pare-feu open source basée sur FreeBSD qui vous offre une gestion sécurisée et efficace du réseau. Notre formation OPNsense vous permettra d'apprendre les bases de l'outil qui intègre des fonctionnalités avancées de routage, de sécurité et de VPN pour protéger les infrastructures.

Pendant ce cours, vous explorerez la configuration des règles de pare-feu, la gestion des VPN pour des connexions sécurisées à distance, ainsi que la surveillance du réseau. Nous apprendrons à configurer les VLANs, analyser le trafic réseau et utiliser le portail captif pour contrôler l'accès.

En plus des bases, des concepts plus avancés seront abordés, tels que la haute disponibilité (HA), l'intégration avec des systèmes d'authentification externes (LDAP, RADIUS) et l'analyse approfondie des logs. L'utilisation d'IDS/IPS pour la détection et la prévention des intrusions sera aussi couverte.

À l'issue de cette formation, vous maîtriserez la configuration et la gestion d'OPNsense, les bonnes pratiques de sécurité réseau, ainsi que les compétences pour protéger les infrastructures d'une PME contre les menaces. Vous saurez aussi diagnostiquer et résoudre des incidents réseaux efficacement.

Cette formation vous sera animée avec les dernières nouveautés concernant l'outil OPNsense.

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

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

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

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de

sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

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.