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

Updated on 18/09/2024

Sign up

OPNsense training

3 days (21 hours)

Presentation

OPNsense is an open source firewall based on FreeBSD, offering secure and efficient network management. Our OPNsense training course will teach you the basics of the tool, which integrates advanced routing, security and VPN features to protect infrastructures.

During this course, you'll explore firewall rule configuration, VPN management for secure remote connections, and network monitoring. We'll learn how to configure VLANs, analyze network traffic and use the captive portal to control access.

In addition to the basics, more advanced concepts will be covered, such as high availability (HA), integration with external authentication systems (LDAP, RADIUS) and in-depth log analysis. The use of IDS/IPS for intrusion detection and prevention will also be covered.

By the end of this course, you'll have mastered OPNsense configuration and management, network security best practices, and the skills needed to protect SMB infrastructures from threats. You'll also know how to diagnose and resolve network incidents effectively.

This training course will bring you up to date with the latest developments in the OPNsense tool.

Objectives

- Understanding the OPNsense interface and benefits
- Install OPNsense on various platforms and configure resources
- Create and manage firewall rules to secure the network
- Configuring and securing NAT and VLANs
- Configure, maintain and optimize VPNs

Target audience

- Network administrators
- Safety managers

Prerequisites

- Basic knowledge of networks (IP, VLAN, routing)
- Understanding the principles of IT security
- Experience with Unix/Linux operating systems (optional, but recommended)
- Familiarity with VPN, NAT and firewall concepts

OPNsense TRAINING PROGRAM

INTRODUCTION TO OPNSENSE

- Introducing OPNsense and its interface
- OPNsense advantages over other firewall solutions
- Typical architecture and key components
- Common use scenarios
- Overview of available add-ons

INSTALLATION AND SIZING

- Hardware requirements and recommendations
- Installation of OPNsense on different platforms (physical, virtual)
- Post-installation: initial configuration and access
- Sizing resources to meet safety requirements
- Setting up an initial backup strategy

FIREWALL RULES MANAGEMENT

- Understand the order of OPNsense processes
- Creating and managing basic filtering rules
- Use aliases to simplify rule management
- Setting up advanced rules and rule groups
- Best practices and firewall security

NAT AND VLAN CONFIGURATION

- Basic and advanced NAT (Network Address Translation) configuration
- Mapping and NAT rule management
- VLAN (Virtual Local Area Network) creation and management
- Securing and isolating traffic with VLANs
- Solving common NAT and VLAN problems

TRAFFIC PRIORITIZATION AND LIMITERS

- Introduction to Quality of Service (QoS)
- Configuring traffic classes and QoS policies
- Setting up limiters to manage bandwidth
- Monitoring and adjusting network performance
- Case studies and simulations

VPN CONFIGURATION

- Overview of VPN types supported by OPNsense (IPsec, OpenVPN, etc.).
- Step-by-step VPN configuration
- Certificate management for secure VPNs
- Best practices for VPN operation and maintenance
- Troubleshooting and optimizing VPN performance

USER MANAGEMENT AND AUTHENTICATION

- Local user configuration and administration rights
- Integration with external authentication systems (LDAP, Active Directory)
- Implementation of security policies for user access
- Monitoring and auditing user activities
- Enhanced security through role management

UPDATES AND MAINTENANCE

- Managing OPNsense System updates
- Planning and applying security patches
- Set up backup and restore routines
- System integrity and performance monitoring
- Incident recovery strategies

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or learning difficulties.

in-company security (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.