

Updated on 03/31/2026

[Sign up](#)

## PacketFence Training

2 days (14 hours)

Our PacketFence training course offers a comprehensive immersion in this open-source network access control (NAC) solution, specifically designed to secure and control connections in heterogeneous environments.

[PacketFence](#) automates the detection and management of network devices, provides role-based access control, and offers captive portals for user authentication, making it an essential tool for network administrators and IT security teams.

Thanks to its compatibility with leading network equipment (Cisco, Aruba, etc.), PacketFence integrates easily into existing infrastructures while enabling granular security management, ranging from anomaly detection to the isolation of suspicious devices.

During this training, you will learn how to install, configure, and manage PacketFence, integrate the solution with your network equipment, and define advanced security policies to better protect your critical resources.

You will also discover how to use PacketFence to monitor incidents in real time and apply automatic penalties for violations of network security policies.

This training will enable you to develop key skills to strengthen the security of your network infrastructure while optimizing the management of users and connected devices.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

# Objectives

- Master the basic principles of PacketFence and its installation
- Manage users, devices, and guests via the captive portal
- Integrate PacketFence with network equipment
- Configure and enforce role-based network security policies
- Monitor and maintain PacketFence

# Target Audience

- Network administrators
- Security engineers
- System and network technicians
- IT Managers

# Prerequisites

- Basic knowledge of TCP/IP networks
- Experience in network management or IT security
- Familiarity with network access concepts (VLAN, 802.1X) and network equipment (switches, routers)
- Experience with RADIUS and LDAP tools is a plus

# OUR PACKETFENCE TRAINING PROGRAM

## Introduction to PacketFence

- Overview of network security and access management
- PacketFence objectives: access control, guest management, device isolation
- History and evolution of PacketFence
- Use cases in network environments
- Key features: anomaly detection, captive portal, integration with network devices
- Technical prerequisites for installing PacketFence

## Installation and initial configuration

- Basic settings: IP addresses, SSL certificates, and DNS
- Network interface configuration (management, isolation, logging)
- Connecting to the PacketFence server and exploring the web administration interface
- Verifying Initial Functionality

## User and device management

- Creating and managing users in PacketFence
- Using roles and permissions for users
- Device management: adding, monitoring, and auditing
- Introduction to the captive portal for user authentication
- Guest Management and Automatic Device Registration
- Using APIs for integration with external systems

## Integration with network equipment

- Integration with switches and access points (Cisco, Aruba, etc.)
- Configuring dynamic VLAN mode for network segmentation
- Introduction to 802.1X and RADIUS management with PacketFence
- Using ACLs for network access management
- Monitoring devices on the network: detection and response
- Troubleshooting connections with network equipment

## Network security and access policies

- Defining security policies based on roles and profiles
- Managing violations and penalties: quarantine, blocking
- Configuring security rules
- Introduction to authentication methods: SSO, LDAP, RADIUS
- Certificate management and advanced security methods
- Implementing real-time monitoring and alerts

## Network monitoring and maintenance

- Using activity logs for monitoring and auditing
- Troubleshooting strategies for PacketFence-related network incidents
- Updating and maintaining PacketFence (patches and new versions)
- Backing up and restoring the PacketFence configuration
- Steps for production deployment and best practices

## Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

## Entry-level requirements

The assessment conducted at the start of the training program complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection issues or

internal security issues within the company (intra-company or virtual classroom) that could hinder the monitoring and smooth running of the training session.

## Teaching Methods

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

## Organization

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

## Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

## Certification

A certificate will be issued to each trainee who has completed the entire training program.