

# Defending the Perimeter from Cyber Attacks Training

Course: **00075**

Filter: **Beginner**

Duration: **4 days**

Category:: **Cyber Security**

Price: **2800,00 €**

## About Course

This Defending the Perimeter from Cyber Attacks course will teach you to ensure the confidentiality, integrity, and availability of your organization's information by protecting your communications and data.

## What you'll learn

- You will learn how to define and implement security principles, install and customize secure firewalls, build Virtual Private Network (VPN) tunnels, and safeguard your organization's network perimeter against malicious attacks.
- Basic security knowledge at the level of: course 468, System and Network Security Introduction
- Working knowledge of TCP/IP and client server architecture

## Pre-requisites

None

## Curriculum

### Module 1: Setting Your Security Objectives

- Defining security principles

- Developing a security policy

## **Module 2: Deploying a Secure Firewall**

- Installing a firewall
- Configuring a firewall to support outgoing services
- Providing external services securely
- Allowing access to internal services

## **Module 3: Detecting and Preventing Intrusion**

- Deploying an IDS
- Detecting intrusions in the enterprise
- Interpreting alerts
- Stopping intruders

## **Module 4: Configuring Remote User Virtual Private Networks (VPNs)**

- Building VPN tunnels
- Deploying client software

## **Module 5: Creating Site-to-Site VPNs**

- Applying cryptographic protection
- Comparing tunneling and protection methods

## **Module 6: Integrating Perimeter Defenses**

- Reducing the impact of denial-of-service (DoS) attacks
- Perimeter architectures