Publication date : 01/19/2024

Course : Check Point R81, network security, level 1

Practical course - 4d - 28h00 - Ref. CPB
Price : 2520 € E.T.

This course will introduce you to the latest version of Check Point products: R81.20. At the end of this course, you will be able to set up and manage a unified security policy (Access Control and Threat Prevention) as well as shared security policies (Geo Policy and HTTPS Inspection).

Teaching objectives

At the end of the training, the participant will be able to:

- Installing and configuring Check Point R81
- Implementing a safety policy
- Implement log review and filtering
- Block intrusions with SAM (Suspicious Activity Monitor)

Intended audience

System/network/security administrators and engineers, technicians.

Prerequisites

Good knowledge of TCP/IP. Basic knowledge of IT security.

Course schedule

1 Operation and installation

- Deployments (distributed, standalone).
- Security Management Server.
- Backup, restore, snapshots and CLI interface.

Hands-on work

Install Check Point under Gaïa in version R81.

PARTICIPANTS

System/network/security administrators and engineers, technicians.

PREREQUISITES

Good knowledge of TCP/IP. Basic knowledge of IT security.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Unified security policy

- Rules, sub-rules by zone.
- Implicit rules, objects with Object Explorer, anti-spoofing.

Hands-on work

Install SmartConsole. Create security objects and policies, shared policies. Manage tags.

3 Address Translation (NAT)

- Rules and RFC 1918.
- NAT static/hide, ARP, VPN.
- Manual, automatic mode.

Hands-on work

Set up automatic NAT (hide, static) and manual transaction rules.

4 Site-to-site and customer-to-site VPN

- Virtual Private Network principles, IPSEC, IKEv1/v2, Software Blade Mobile Access.
- Traditional and simplified modes.
- Endpoint Security Heavy Client, Check Point Mobile.
- Mobile Access authentication: Check Point Mobile, iOS/Android clients, SSL Network Extender (SNX) captive portal.

Hands-on work

Set up a site-to-site IPSec tunnel, remote access using IPSec VPN. Activate and set up Check Point Mobile.

5 Firewall and user management

- Manage Smartcenter logs and alerts.
- Logs & Monitor, Gateways & Servers tabs.
- SAM (Suspicious Activity Monitor) features with Check Point SmartView Monitor R81.
- User authentication.
- Identity Collector management.
- Using Access Roles.

Hands-on work

Implement Identity Awareness, log review and filtering. Blocking intrusions with SAM.

6 IPS module

- Vulnerabilities, security flaws, CVE referencing.
- Security profile, IPS policy.

Example

Protection against vulnerabilities with the IPS module.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 Application control

- Notions of application signatures.
- Creation of customized applications.
- Management of limits, UserCheck, URL filtering.

Example
Deployment of a content security policy.

8 Threat Prevention

- Antivirus and Antibot modules.
- Threat Extraction/Emulation.

Hands-on work
Implementation of a Threat Prevention policy.

Dates and locations

REMOTE CLASS
2026 : 10 Mar., 16 June, 27 Oct.

PARIS LA DÉFENSE
2026 : 10 Mar., 16 June, 27 Oct.