Course : Check Point R82, Network Security, Level 1

Practical course - 4d - 28h00 - Ref. CPG
Price : 3030 CHF E.T.

NEW

This course will introduce you to the latest version of Check Point products: R82. 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 R82
- ✓ Deploy a security policy and monitor traffic
- ✓ Deploy remote sites and share security policies
- ✓ Mastering log visualization and monitoring
- ✓ Manage user authentication
- ✓ Implementing a high-availability cluster

Intended audience

System/network/security administrators and engineers, technicians.

Prerequisites

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

Course schedule

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.

1 Gaia deployment: installation of [appliances " Check Point

- Check Point products.
- New features in versions R81.xxx and R82.
- Introducing the Gaïa system.
- Elements of three-tier architecture.
- Modular software blade architecture.
- Check Point Infinity.
- Distributed and standalone architecture.
- The management server. SIC protocol.

Hands-on work

Installation of Check Point R82.

2 Security Management Server, unified management tool Smart Console

- SIC protocol communication and object management.
- Getting started with SmartConsole R82.
- Security policy. Rules management.
- Unified policies.
- Package inspection.
- "Inline" Policies (under rules).
- SmartConsole Web.

Hands-on work

SmartConsole installation. Create objects. Create a security policy.

3 Address Translation (NAT)

- Address translation rules for IPv4 and IPv6.
- Static NAT (One To One NAT) and dynamic NAT (.Many To One NAT)/PAT.
- Manual NAT.
- ARP and routing.

Hands-on work

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

4 Multi-site management

- Definition of Policy Packages.
- Policy Packages management.
- Definition and types of layers.
- Inspection of packets in an ordered layer.
- Policy Layers Sharing.
- Administrator management in SmartConsole.
- Communication with the remote Gateway.

Hands-on work

Set up a remote gateway, create a security policy (Policy Pack) and basic rules for the remote site. Create and share an ordered layer. Create a new permission profile with limited authorizations.

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.

5 Logs and monitoring

- Log management policy.
- Track connections with logs and monitor (old SmartView Tracker).
- The Monitor.
- Log management.
- SmartView Monitor, functions and warning thresholds.
- Dedicated log server.

Hands-on work

Monitoring : utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l'état de la politique de sécurité. Troubleshooting : accéder au mode expert, aux commandes "tcpdump" et "fw ctl zdebug drop", visualiser et manipuler les utilitaires CPView et Top.

6 HTTPS decryption

- Creation of outbond and inbound rules.
- Certificate management.
- Server Name Indications (SNI).
- Management of advanced tools in SmartConsole.
- Introduction to learning mode and performance prediction.
- Introducing Client Side Fail mode.
- Introducing the Bypass under load feature.
- Supports HTTP/3 streams with QUIC (UDP) transport protocol.

Hands-on work

Implement HTTPS inspection.

7 Application control/URL filtering

- The limits of a classic firewall by IP and port.
- Application recognition.
- Access control.
- The "AppWiki". URL Filtering.
- The user check.
- DNS filtering with the Advanced DNS blade.
- User-based policy.
- Recover user identity, Identity Awareness authentication methods.

Hands-on work

Filtrage web et applications : créer et partager la politique de Filtrage Web et Applications en tant que inline layer et ordered layer. Authentification : mise en place d’Identity Awareness, création de rôles et des accès.

8 IPSec site-to-site VPN and remote access

- VPN architecture.
- Encryption basics, introduction to IKE and IPSec.
- Certification Authority (CA). Domain-Based VPN.
- Simplified mode. VPN community configuration.
- VPN routing.
- Use the new Network Probe object to monitor the status of VPN tunnels.
- SSL VPN and IPSec VPN.
- Blade Mobile Access.
- Mobile Access type: Remote Access.
- Endpoint Security VPN.
- NAT-Traversal, Visitor Mode, Hub Mode and Office Mode.

Hands-on work

VPN-IPSec Inter-sites (Shared Secret). VPN-IPSec Intersites (certificates). Remote access VPN connection via Check Point Mobile client, also for Active Directory users.

9 Threat Prevention Policy

- Threat Prevention policy and software blades.
- Rules management.
- Safety profiles.
- Presentation of AI-based prevention engines: ThreatCloud Graph, Kronos, Deep Brand Clustering.
- Introduction of autonomous Threat Prevention.
- Automatic Zero Phishing Configuration.
- Feature "Adaptive Hold" for Anti-Virus and Anti-Bot blades.

Hands-on work

Anti-Virus and Anti-Bot.

10 Clustering

- Firewall redundancy.
- ClusterXL in High Availability mode.
- ClusterXL in load sharing mode.
- ClusterXL in Active-Active mode.
- VMAC and ARP issues.

Hands-on work

Implementation of ClusterXL in High Availability mode.

Dates and locations

REMOTE CLASS

2026 : 10 Mar., 2 June, 15 Sep., 24 Nov.