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

Updated on 02/10/2025

Sign up

CCSA certification training

ALL-IN-ONE: EXAM INCLUDED IN PRICE

4 days (28 hours)

Presentation

CCSA (Check Point Certified Security Administrator) certification is a benchmark in cybersecurity. It validates the ability to deploy, configure and administer a Check Point solution in an enterprise environment.

Our CCSA training will enable you to master policy management, VPN configuration, address translation (NAT), monitoring and implementation of high-availability architectures.

You'll apply diagnostic tools and advanced modules (IPS, Anti-Virus, Anti-Bot) for operational protection.

Through a resolutely practical approach, you'll consolidate the skills needed to secure modern networks, while preparing for CCSA R81.x certification.

Like all our training courses, this one is based on the latest stable version of the Check Point ecosystem, and focuses on real-life situations.

Objectives

- Manage an end-to-end Check Point infrastructure.
- Design and deploy effective security policies.
- Configure and troubleshoot site-to-site and remote access VPNs.
- Ensure high availability and resilience.
- Use monitoring and troubleshooting tools.
- Pass the CCSA R81.x exam.

Target audience

- System and network administrators
- Security / SOC engineers and analysts
- Security consultants and technicians

Prerequisites

- Basic knowledge of TCP/IP and security
- First experience with a firewall

CCSA training program

[Day 1 - Morning]

Introduction to the Check Point ecosystem and certification

- Overview of Check Point solutions and R81.x versions
- TCP/IP network reminders and stateful firewall principles
- Security Gateway and Security Management architecture
- Discover SmartConsole and the main blades
- Practical workshop: First connection, inventory and menu navigation.

[Day 1 - Afternoon]

Objects, policies and deployment

- Creating network, service and user objects
- Designing a robust security policy
- Managing policy installations and sessions
- Best practices for segmentation and hardening
- Practical workshop: Writing, validating and deploying an initial policy.

Access control and identity

- LDAP/RADIUS/TACACS+ integration and Identity Awareness
- User/group-based rules and application controls
- Authentication logs, correlation and auditing
- Caveats: inheritance, dynamic groups, priorities
- Practical workshop: Conditional access by AD group.

[Day 2 - Morning]

Address Translation (NAT) and flows

- NAT models: static, dynamic, hide NAT
- Rule evaluation order and collision resolution
- Log reading and flow tracing
- Common pitfalls: asymmetry, ephemeral ports, PAT
- Practical workshop: NAT scenarios and connectivity validation.

[Day 2 - Afternoon] Logs,

visibility and detection

- SmartLog and SmartEvent operation
- Advanced searches, reports, dashboards
- Alerting and SIEM integration
- Traceability and compliance: retention and backups
- Practical workshop: End-to-end incident analysis.

Site-to-site VPN and remote access

- IPsec concepts (phases, crypto, PFS, lifetimes)
- Site-to-site VPN configuration
- Remote Access VPN: profiles, client deployment
- Troubleshooting: IKE negotiation, interesting selection, routing
- Practical workshop: setting up an inter-site tunnel.

[Day 3 - Morning]

High availability and ClusterXL

- HA and Load Sharing modes, topologies and prerequisites
- ClusterXL configuration and state synchronization
- Failover tests and application validation
- Maintenance: packages, upgrades, change windows
- Practical workshop: two-node cluster and controlled failover.

[Day 3 - Afternoon]

Threat prevention and advanced security

- IPS, Anti-Bot, Anti-Virus, App Control, URL Filtering modules
- Profiles, exceptions, updates and performance
- HTTPS (TLS) traffic inspection: impacts and best practices
- Threat analysis and response
- Practical workshop: Hardening an environment against a simulated attack.

Administration and governance

- Administrative roles, permissions and delegation
- Backup/restore, snapshots, configuration export
- License and support management
- Compliance & global policies
- Practical workshop: Backups and disaster recovery.

[Day 4 - Morning]

Troubleshooting and analysis tools

- Troubleshooting methodology
- Tools: cpview, tcpdump, fw monitor
- VPN/NAT/HA diagnostics: typical cases
- Collecting support archives and best practices
- Practical workshop: Guided resolution of multi-domain incidents.

[Day 4 - Afternoon]

Production start-up and operation

- Go-live checklist: security, backups, supervision
- Upgrade and maintenance strategies
- Cloud/hybrid integration and segmentation
- Performance measurement and capacity planning
- Practical workshop: Operations runbook and dashboard.

Preparation for CCSA R81.x certification

- Exam format, key topics and weighting
- Revision strategies, pitfalls and time management
- Official resources and labs
- Personalized action plan
- Practical workshop: Mock exam + correction.

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 confirmed, the learner receives a self-assessment questionnaire enabling us to

assess the learner's estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 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 is used to check that skills have been correctly acquired.

Certification

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