Check Point Certified Security Administration (CCSA) Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

The **Check Point Certified Security Administration (CCSA)** training program provides IT and cybersecurity professionals with the essential knowledge and practical skills required to deploy, configure, and manage **Check Point Next Generation Firewalls (NGFWs)**. Designed for organizations seeking stronger network security and centralized policy management, this course covers the core technologies used to protect modern enterprise environments.

Throughout the course, participants will gain hands-on experience with **Check Point Security Gateway**, **SmartConsole**, **Gaia Operating System**, **Application Control**, **URL Filtering**, **NAT**, **VPN**, **Threat Prevention**, and **Infinity Threat Protection** technologies. Learners will also explore traffic visibility, threat detection, security monitoring, and advanced network protection techniques.

This training prepares participants for the **CCSA (Check Point Certified Security Administrator)** certification while developing practical skills applicable in real-world enterprise security environments.

Prerequisites

To gain maximum benefit from this course, participants should have:

- General knowledge of **TCP/IP**
- Understanding of networking technologies
- Familiarity with Windows and UNIX/Linux operating systems
- Basic knowledge of Internet technologies and network infrastructure

Who Should Attend

This course is ideal for:

- **System Administrators**
- **Network Engineers**
- **Security Administrators**
- **Support Analysts**
- **Security Managers**
- Security Operations personnel
- Network security professionals
- Technical staff managing Check Point solutions
- Professionals preparing for **CCSA Certification**

Check Point Certified Security Administration (CCSA) Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, learners will be able to:

- Understand **Check Point Security Architecture**.
- Manage systems using the **Gaia Operating System**.
- Create and deploy security policies using **SmartConsole**.
- Manage user access and authentication.
- Configure **Application Control** and **URL Filtering**.
- Implement manual and automatic **NAT** policies.
- Deploy and manage secure VPN connections.
- Monitor network traffic and security events.
- Configure and maintain **Threat Prevention** technologies.
- Utilize **Infinity Threat Protection** capabilities.
- Implement security controls for IoT environments.

Training Outline

Check Point Security Architecture

Introduction to Network Security

- **Check Point Security Architecture**
- Network security fundamentals
- Security layers and controls
- Secure network design principles
- Overview of Check Point products

Security Gateway Components

- Security Gateway architecture
- Traffic inspection processes
- Policy enforcement mechanisms

Gaia Operating System

Gaia Fundamentals

- **Gaia Operating System**
- System administration
- Network configuration
- Administrative tools
- System maintenance and updates

SmartConsole Management

SmartConsole Fundamentals

- **SmartConsole**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Administrative interface navigation
- Security policy creation
- User and access management
- Reporting and management tools

Browser SmartConsole

- Web-based administration
- Centralized management workflows
- Policy deployment processes

Licensing and Product Management

License Administration

- Check Point licensing models
- Support and maintenance agreements
- Product activation
- Software updates and lifecycle management

Security Policy Management

Security Policies

- Creating and managing security policies
- Rule management
- Policy enforcement
- Security auditing

Policy Layers

- **Policy Layer Concepts**
- Layered security models
- Policy optimization
- Rule hierarchy management

Application and Web Security

Application Control

- **Application Control**
- Application-aware security policies
- Blocking high-risk applications
- Application visibility and monitoring

URL Filtering

- **URL Filtering**
- Web access policies
- Content filtering
- Category-based access control

Check Point Certified Security Administration (CCSA) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

NAT and Network Access

Network Address Translation

- **Static NAT**
- **Hide NAT**
- Manual NAT configurations
- Automatic NAT deployment

VPN Administration

Virtual Private Networks

- **VPN Fundamentals**
- Secure remote access
- Site-to-site VPN implementation
- VPN configuration and management
- Encryption and security policies

Network Monitoring and Visibility

Monitoring and Traffic Visibility

- Traffic visibility and analytics
- Network performance monitoring
- User activity tracking
- System health monitoring

Monitoring States

- System status management
- Event monitoring
- Performance improvement tools

Threat Prevention and Security Operations

Threat Prevention

- **Threat Prevention**
- Attack detection and prevention
- Threat mitigation strategies
- Security event analysis

Intrusion Prevention System (IPS)

- IPS configuration and management
- Threat signatures
- Security tuning
- Performance optimization

Threat Extraction and Threat Emulation

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Threat Extraction**
- **Threat Emulation**
- Malware analysis
- Advanced threat protection

Infinity Threat Protection

Infinity Security Platform

- **Infinity Threat Prevention**
- Multi-layered security architecture
- Threat intelligence integration
- Centralized security management

IoT Security

IoT Protect

- **Check Point IoT Protect**
- IoT device visibility
- IoT risk management
- Network segmentation
- Industrial device security

Security Events and Analysis

Security Event Management

- Security event monitoring
- Log management
- Incident response processes
- Security reporting and analytics

CCSA Certification Preparation

- Certification exam objectives
- Core Check Point technologies
- Hands-on lab exercises
- Real-world security scenarios
- Exam preparation strategies