

# Check Point Certified Security Administrator (CCSA) R81.20

Kód kurzu: CCSAR

Tento základní kurz se zabývá základy potřebnými pro nasazení, konfiguraci a správu každodenního provozu bezpečnostních bran a Managementu Check Point na operačním systému Gaia.

Pobočka	Dnů	Cena kurzu	ITB
Praha	3	33 500 Kč	0
Bratislava	3	1 457 €	0

Uvedené ceny jsou bez DPH.

## Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
17.02.2025	3	33 500 Kč	Prezenční	CZ/SK	Gopas Praha Přeprdej prezenční
<b>G</b> 17.02.2025	3	1 457 €	Online	CZ/SK	Gopas Bratislava Přeprdej online
28.04.2025	3	33 500 Kč	Prezenční	CZ/SK	Gopas Praha Přeprdej prezenční
28.04.2025	3	33 500 Kč	Online	CZ/SK	Gopas Praha Přeprdej online
28.04.2025	3	1 457 €	Online	CZ/SK	Gopas Bratislava Přeprdej online

Uvedené ceny jsou bez DPH.

## Pro koho je kurz určen

Technical professionals who support, install deploy or administer Check Point products.

## Co Vás naučíme

- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Explain how communication is secured and how traffic is routed in the Check Point environment.
- Describe the basic functions of the Gaia operating system.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.
- Explain how policy layers affect traffic inspection.
- Articulate how Network Address Translation affects traffic.
- Describe how to configure manual and automatic Network Address Translation (NAT).
- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third party and externally managed VPN Gateways.
- Describe how to analyze and interpret VPN tunnel traffic.
- Configure logging parameters.
- Use predefined and custom queries to filter log results.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.

### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Check Point Certified Security Administrator (CCSA) R81.20

## Požadované vstupní znalosti

Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.

## Studijní materiály

Studijní materiál Check Point.

## Osnova kurzu

### Topics:

- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contract
- Policy Rule and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation

### Exercises:

- Deploying SmartConsole
- Installing a Security Management Server
- Installing a Security Gateway
- Configuring Objects in SmartConsole
- Establishing Secure Internal Communication
- Managing Administrator Access
- Managing Licenses
- Creating a Security Policy
- Configuring Order Layers
- Configuring a Shared Inline Layer
- Configuring NAT
- Integrating Security with a Unified Policy
- Elevating Security with Autonomous Threat Prevention
- Configuring a Locally Managed Site-to-Site VPN
- Elevating Traffic View
- Monitoring System States
- Maintaining the Security Environment

#### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved