Check Point Security Administrator R81.10 (CCSA)

Check Point

Live Training (também disponível em presencial)

- **Localidade:** Lisboa
- **Data:** 27 Jun 2022
- **Preço:** 1910 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das das 9h00 às 17h00
- **Nível:** Avançado
- **Duração:** 21h

Sobre o curso

Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.

Three-day course covers everything you need to start-up, configure and manage daily operations of R81.10 Check Point Security Gateway and Management Software Blades systems on the GAiA operating system.

Learn How To:

- Install R81.1 management and a security gateway in a distributed environment
- Configure objects, rules, and settings to define a security policy
- Work with multiple concurrent administrators and define permission profiles
- Configure a Virtual Private Network and work with Check Point clustering
- Perform periodic administrator tasks as specified in administrator job descriptions

How You Will Benefit:

- Be prepared to defend against network threats
- Evaluate existing security policies and optimize the rule base
- Manage user access to corporate LANs
- Monitor suspicious network activities and analyze attacks
- Implement Check Point backup techniques

Destinatários

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

Objetivos

- Know how to perform periodic administrator tasks.
- Describe the basic functions of the Gaia operating system.
- Recognize SmartConsole features, functions, and tools.
- Understand how SmartConsole is used by administrators to give user access.
- Learn how Check Point security solutions and products work and how they protect networks.
- Understand licensing and contract requirements for Check Point security products.
- Describe the essential elements of a Security Policy.
- Understand the Check Point policy layer concept.
- Understand how to enable the Application Control and URL Filtering software.
- Use Blades to block access to various applications.
- Describe how to configure manual and automatic NAT.
- Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements.
- Describe different Check Point Threat Prevention solutions for network attacks.
- Articulate how the Intrusion Prevention System is configured, maintained and tuned.
- Understand the Infinity Threat Prevention system.
- Knowledge about Check Point’s IoT Protect

Pré-requisitos

- Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP

Metodologia

- Sessões teóricas e práticas.

Programa

- Security Architecture
- Application Control
- Deployment
- Licensing
- Gaia Portal
- Hide/Static NAT
- URL Filtering
- Monitoring States
- IoT
- Traffic Visibility
- Security Events
- Threat Emulation
- Policy Layers
- Browser SmartConsole
- Infinity Threat Prevention
- User Access

LAB EXERCISES

- Configure the Security Management Server.
- Use the WebUI to run the First Time Wizard.
- Install the Smart Console.
- Install the Alpha Gateway using the network detailed in the course topology.
- Demonstrate how the Security Management Server and Gateway communicate.
- Test SIC Status.
- Create multiple administrators and apply different roles and permissions for simultaneous administration.
- Validate existing licenses for products installed on the network.
- Create and configure host, network and group objects.
- Create a simplified Security Policy.
- Demonstrate how to use Security Zones in policy.
- Demonstrate how to share a layer between Security Polices.
- Configure Network Address Translation for server and network objects.
- Enable Identity Awareness.
- Deploy user access roles for more granular control of the security Policy.
- Generate network Traffic and use traffic visibility tools to monitor the data.
- Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.