Check Point Security Expert R81.20 (CCSE)

Check Point

- **Nível:** Avançado
- **Duração:** 21h

Sobre o curso

Learn advanced concepts and develop skills necessary to design, deploy, and upgrade Check Point Security environments.

Advanced three-day course teaches how to build, modify, deploy and troubleshoot the R81.20 Check Point Security Systems on the GAiA operating system. Hands-on lab exercises teach how to debug firewall processes, optimize VPN performance and upgrade Management Servers.

Destinatários

Technical Professionals who architect, upgrade, maintain, and support Check Point products.

Objetivos

- Identify basic interfaces used to manage the Check Point environment.
- Identify the types of technologies that Check Point supports for automation.
- Explain the purpose of the Check Management High Availability (HA) deployment.
- Identify the workflow followed to deploy a Primary and solution Secondary servers.
- Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, connection stickyness.
- Identify how to exclude services from synchronizing or delaying synchronization.
- Explain the policy installation flow.
- Explain the purpose of dynamic objects, updatable objects, and network feeds.
- Understand how to manage user access for internal and external users.
- Describe the Identity Awareness components and configurations.
- Describe different Check Point Threat Prevention solutions.
- Articulate how the Intrusion Prevention System is configured.

- Obtain knowledge about Check Point’s IoT Protect.
- Explain the purpose of Domain-based VPNs.
- Describe situations where externally managed certificate authentication is used.
- Describe how client security can be provided by Remote Access.
- Discuss the Mobile Access Software Blade.
- Explain how to determine if the configuration is compliant with the best practices.
- Define performance tuning solutions and basic configuration workflow.
- Identify supported upgrade and migration methods and procedures for Security Management Servers and dedicated Log and SmartEvent Servers.
- Identify supported upgrade methods and procedures for Security Gateways.

Pré-requisitos

CCSA Training or Certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

Metodologia

- Sessões teóricas e práticas

Programa

COURSE TOPICS

- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Performance Tuning
- Advanced Security Maintenance

LAB EXERCISES

- Navigate the Environment and Using the Management API
- Deploy Secondary Security Management Server
- Configure a Dedicated Log Server
- Deploy SmartEvent
- Configure a High Availability Security Gateway Cluster
- Work with ClusterXL
- Configure Dynamic and Updateable Objects
- Verify Accelerated Policy Installation and Monitoring Status
- Elevate Security with HTTPS Inspection
- Deploy Identity Awareness
- Customize Threat Prevention
- Configure a Site-to-Site VPN with an Interoperable Device
- Deploy Remote Access VPN
- Configure Mobile Access VPN
- Monitor Policy Compliance
- Report SmartEvent Statistics
- Tuning Security Gateway Performance