



Check Point Security Engineering and Troubleshooting Expert R81.20 (CCSE+CCTE)

Check Point

- **Nível:**
 - **Duração:** 35h
-

Sobre o curso

This 5-day course combines the [Check Point Security Engineering \(CCSE\)](#) and the [Check Point Troubleshooting Expert \(CCTE\)](#) courses.

This course :

- teaches how to build, modify, deploy and troubleshoot Check Point Security Systems on the GAIa operating system. The Hands-on lab exercises teach how to debug firewall processes, optimize VPN performance and upgrade Management Servers.
 - provides advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point security environment.
-

Destinatários

- Expert users and resellers who need to perform advanced deployment configurations of Check Point Software Blades.
 - Security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.
-

Pré-requisitos

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

- Working knowledge of UNIX and/or Windows operating systems
 - Working knowledge of Networking TCP/IP
 - CCSE training/certification
 - Advanced knowledge of Check Point Security products
-

Metodologia

- Sessões teóricas e práticas.
-

Programa

COURSE TOPICS ENGINEERING

- 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 ENGINEERING

- 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

COURSE TOPICS ADVANCED TROUBLESHOOTING

- Introduction to Advanced Troubleshooting
- Advanced Management Server Troubleshooting
- Advanced Troubleshooting with Logs and Events
- Advanced Gateway Troubleshooting
- Advanced Firewall Kernel Debugging
- Advanced Access Control Troubleshooting
- Advanced Identity Awareness Troubleshooting
- Advanced Site-to-Site VPN Troubleshooting
- Advanced Client-to-Site VPN Troubleshooting

LAB EXERCISES ADVANCED TROUBLESHOOTING

- Collect and read live and historical CPView data.
- Troubleshoot CPM and SmartConsole login issues.
- Restore a Management High Availability environment from a temporary Primary Down condition.
- Troubleshoot SmartLog processes.
- Collect and interpret user mode debugs.
- Collect and interpret kernel debugs.
- Debug Unified Policy Inspection in kernel to understand match process.
- Debug the Identity Awareness user mode processes.
- Collect and interpret Site-to-Site VPN Debugs.
- Collect and interpret Remote Access VPN Debugs