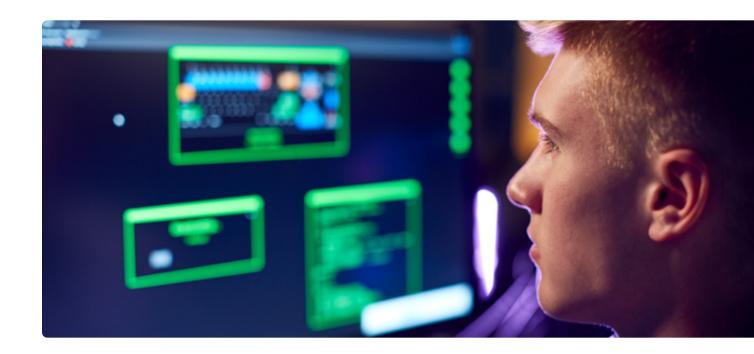# Check Point R81

ONLINE TRAINING COURSE

Course description

The Checkpoint R81 training (Check Point Certified Security Administrator) at InfosecTrain has been designed to provide a detailed knowledge of the basic concepts and the skills, that are required to configure Check Point Security Gateway and to Managing Software Blades. Our trainers are the experts of the Industry and they assure to enhance the knowledge of the candidates on managing the complexities and threats posed on the network of an organisation. Our Checkpoint CCSA certification course focuses on:

• Preparing the participants to defend against network threats

• Teaching evaluation of existing security policies and optimizing the rule base

• Training to manage user access to corporate LANs

The key features of the training are:

• Training by the experts of the domain.

• In-depth knowledge sharing on each domain of the exam.

• Custom made training available

• Multiple practice papers to get acquainted with the exam format.

Target Audience

CheckPoint R81 Training is most beneficial for

• System administrators
• Security managers
• Network engineers
• Analysts

Prerequisites

Candidate who are interested in this training must have

• Basic knowledge of networking

• And it is also recommended to have 6 months to 1 year of experience with Check Point products

Why Infosec Train?

Certified & Experienced Instructor	Flexible Schedule	Access to the recorded sessions
Post Training Support	Tailor Made Training	4 hrs/day in Weekend/ Weekday

Course Content

INFOSECTRAIN

1. NGFW overview & CheckPoint Features

- Why do we need Firewall in spite of ACL in Router
- Stateful Inspection
- CheckPoint UTM Features

2. CheckPoint Components Overview

- Firewall / Gateway/ Enforcement Module (NG Appliances)
- Management Server (Smart-1 Appliances)
- Smart Console or GUI client
- Log Server

3. CheckPoint Installation Scenarios

- Standalone Installation (2 Tier)
- Distributed Installation (3 Tier)
- Standalone vs Distributed

4. CheckPoint Standalone (2-Tier) Installation

- Installation of CheckPoint ISO (FW + Management) at 9HQ site) in PNET environment
- Installation of Smart Console on Windows PC
- Enabling Blades on CheckPoint Objects
- Configure Network Interfaces & Topology (Anti-Spoofing concept)
- Configure Routing (static & Default Routes)
- Login to the Console and install Default Policy

5. CheckPoint Distributed (3-Tier) Installation

- Installation of CheckPoint ISO (FW) on PNET environment at (HQ site)
- Installation of CheckPoint ISO (Management) on PNET environment (HQ Site)
- Adding a Gateway to the Security Management Server (SIC Integration)
- SIC Troubleshooting
- Expert Mode & CLISH

6. Managing Administrators & GUI Clients

- Manage GUI Client via Web &CLI
- Add Permission Profile
- Add Administrator and Add Permission Profile
- Database Lock concepts

7. Policies

- Add a WAN Firewall to Management Server at (WAN site)
- Add a Policy for WAN Firewall on Management Server (HQ site)
- Add a Policy for Core to WAN Firewall connectivity
- Policy Objects (Nodes, Host, Network, Groups, Address Ranges, Services etc.)
- Add Internet Access Rule
- Add FW Management Rules
- Add DMZ Access Rules
- Policy Layers (Introduction)
- Ordered Layers and Inline Layers
- Shared Layers
- Policy Optimization for performance
- Implied rules & Global Properties
- Stealth Rule, Clean-up Rule
- Database Revision Control

8. Logs Management and Adminsitration

- Log Files & Troubleshootin (Filters, etc)
- Log files Management

9. Network Address Translation

- NAT Theory & Concepts
- Auto NAT (Hide & Static) Lab
- Manual NAT (Hide & Static) Lab
- PAT Concepts
- No-NAT Concept

10. CheckPoint Clustering

- Add Cluster object
- Add Cluster Members
- Configure Clustering
- Test Clustering
- High-Availabilitiy and Load Sharing scenarios

11. HTTPS Inspection

- SSL Concept & HTTPS Inspection
- Configure HTTPS Inspection
- Generate HTTPS Cerificate and install the Certificate on Nodes
- Enable HTTPS Inspection Blade & Deploy Policy for SSL Decrytion
- Test SSL Decryption

12. UTM Features

- Application Control
- URL filtering
- Content Awareness
- DLP
- Threat Prevention Policy (Concept and Overview)
- IPS (Concept and overview)
- Infinity Protection

13. Identity Awareness

- User based Access rule with authenticated Access
- Client Authentication
- External Authentication for Users (RADIUS /TACACS)
- Install AD server at Site-b
- Enable Identity Awareness Blade
- Configure Identity Awareness rules based on Access objects

14. VPN

- VPN Theory
- VPN Site-A to Site-B configuration (Lab)
- Remote Access VPN
- Mobile Access / SSL VPN
- VPN tunnel Utility

15. Backup & Restore

- Backup, Restore & Snapshot through Web GUI
- Backup, Restore & Snapshot through CLI

16. Command Line Interface (Introduction & Basic Commands)

- cpconfig
- cpstop and cpstart commands, cprestart
- configure interfaces
- configure routes
- Some More commands

www.infosectrain.com | sales@infosectrain.com