

Check Point Security Administration I NGX (R65)

Introduction

This course prepares the participants to appear for the certification exam **CCSA NGX R65**

Check Point Security Administration I NGX (R65) – CCSA NGX is a foundation level certification that validates a candidate's ability to configure and manage fundamental implementations of Check Point's flagship product, VPN-1 (NGX R65), as an enterprise level Internet security solution to protect corporate networks. As a CCSA NGX, security professionals possess the requisite skills to define and configure security policies that enable secure access to information across corporate networks. In addition to these essential skills, CCSA NGX professionals also have the ability to monitor network security activity and implement measures to block intruder access to networks.

Duration

3 Days

Prerequisites

Basic networking knowledge and working knowledge of Windows Server operating system and experience with TCP/IP and Internet technologies

Who Should Attend?

Systems administrators, security managers, and network engineers who manage VPN-1 NGX gateway deployments, and individuals seeking the Check Point Security Administration NGX (CCSA NGX) certification

Course Objectives

➤ Introduction to VPN-1

- Given your understanding of Check Point's three-tier architecture and basic firewall concepts, design and install a distributed deployment of VPN-1.
- Test to verify the VPN-1 deployment, based on SIC establishment between the SmartCenter Server and the Gateway using SmartDashboard.

➤ Introduction to SecurePlatform

- Given the most current configuration, update the appropriate network interface using the sysconfig utility to change the management interface.
- Given specific instructions, perform a backup and restore of the current Gateway installation from the command line.

➤ Introduction to the Security Policy

- Given the network topology, create and configure network, host, and gateway objects for your city site.
- In SmartMap view, actualize your city site's network objects.
- In SmartMap, given your partner city's network data, create and configure your partner city's Web server object.
-
-

Check Point Security Administration I NGX (R65) – Contd.

- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use. Test your Rule Base with your partner city, and evaluate logs in SmartView Tracker.
- Given your Policy's implicit rules, configure an implied rule for logging purposes.
- Manually configure NAT rules on your Web-server and Gateway objects. Refer to the Global Properties of the Gateway object.
- Configure the Policy using Database Revision Control.

➤ **Monitoring Traffic and Connections**

- Given a deployment strategy, test and verify a new Policy using SmartView Tracker.
- Given evidence of a potential intrusion or attack using SmartView Tracker, change the Policy to block the offending connection.
- Use SmartView Monitor to block and monitor a user's activities by implementing the SAM rule.
- Given accumulated raw-logged data, configure Eventia Reporter to monitor and audit network traffic.

➤ **Authentication**

- Create and configure users in SmartDirectory for access to your LAN.
- Modify your Rule Base to provide permissions for users.
- Configure partially automatic Client Authentication, and install, test, and verify the Policy in SmartView Tracker.

➤ **Check Point QoS**

- Given a distributed network deployment, design a strategy for implementing QoS.
- Based on an implementation of QoS, configure the required bandwidth allocation for the network.

➤ **Basic SmartDefense and Content Inspection**

- Using content inspection, Application Intelligence, and/or Web Intelligence, configure for port scanning and HTTP worm catcher.
- Create a SmartDefense profile, and incorporate port-scanning and successive-events settings into the profile. Test the configuration with your partner city's Web server, and evaluate logs using SmartView Tracker.
- Block connections, given evidence of a potential intrusion or attack. Evaluate logs.
- Based on network analysis disclosing threats by specific sites, configure a Web-filtering and antivirus Policy to filter and/or scan the threatening traffic.