

CPX-001 Check Point Security Administration NGX I (CCSA NGX)

Duration: 2 days (9:00 am to 5:00 pm)

Course Description

Check Point Security Administration NGX I is a foundation course for Check Point's flagship product, VPN-1/FireWall-1. This course covers configuring VPN-1/FireWall-1, and provides hands-on training managing a VPN-1/FireWall-1 installation. With over 24,000 CCSA certified professionals worldwide, CCSA NGX certification is one of the most highly recognized and respected vendor-specific security certifications available. The foundation of Check Point certifications, CCSA NGX certification validates a Security Administrator's ability to maintain day-to-day operation of Check Point security solutions and ensure secure access to information across the network. Proficiencies include creating and installing security policies, using logging and reporting features, and managing anti-spoofing, Network Address Translation (NAT), and OPSEC applications.

You will learn:

- ◆ VPN-1/FireWall-1 architecture
- ◆ VPN-1/FireWall-1 component deployment
- ◆ How to define a Security Policy using SmartDashboard
- ◆ How to deploy and manage distributed gateways, using Check Point's SmartUpdate and Secure Internal Communications
- ◆ How to administer and troubleshoot VPN-1/FireWall-1 Security Policies
- ◆ How to enable SmartDefense global protection mechanisms
- ◆ How to set up User Authentication in a VPN-1/FireWall-1 environment
- ◆ How to implement Network Address Translation
- ◆ How to protect your network with backups
- ◆ How to upgrade VPN-1/FireWall-1
- ◆ How to license VPN-1/FireWall-1

Lab Exercises:

- ◆ Defining VPN-1/FireWall-1 rules, objects, and users
- ◆ Establishing basic VPN-1/FireWall-1 Security Policies
- ◆ Setting up User Authentication
- ◆ Configuring SmartDefense
- ◆ Configuring Network Address Translation
- ◆ Using SmartUpdate for VPN-1/FireWall-1 installation

Target Audience

- ◆ Systems administrators, security managers, or network engineers managing VPN-1/FireWall-1 gateway deployments.
- ◆ Individuals seeking the Check Point Security Administration (CCSA) NGX certification.

Course Objectives

- ◆ Manage network security with VPN-1 NGX
- ◆ Create rules and modify a Security Policy's properties
- ◆ Use monitoring tools to track, monitor, and account for all connections logged by Check Point components
- ◆ Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations
- ◆ Protect organizations from known network attacks and entire categories of emerging or unknown attacks, using SmartDefense
- ◆ Distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports
- ◆ Verify the identity of users logging in to VPN-1 NGX, using VPN-1 NGX authentication schemes
- ◆ Implement LDAP and integrate it with VPN-1 NGX SmartCenter Server
- ◆ Configure VPNs, using IKE encryption and Check Point's simplified VPN setup
- ◆ Back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers

Course Outline

Chapter 1: Check Point Security Administration NGX I

- ◆ Course Objectives
- ◆ Course Layout
 - Prerequisites
 - Check Point Certified Security Administrator (CCSA)
 - Recommended Setup for labs

Chapter 2: VPN-1 NGX Overview

- ◆ Objectives
- ◆ Key Terms
- ◆ How VPN-1 NGX Works
 - The INSPECT Engine
- ◆ VPN-1 NGX Architecture
 - SmartConsole
 - SmartDashboard
 - SmartCenter Server
 - Security Gateway
- ◆ Distributed Deployments
 - SVN Foundation
 - Secure Internal Communications (SIC)
- ◆ Lab 1: NGX Stand-Alone Installation
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 3: The Security Policy

- ◆ Objectives
- ◆ Key Terms
- ◆ Security Policy Defined
 - What is a Security Policy?
 - Security Policy Considerations
- ◆ Rule Base Defined
- ◆ Lab 2: Launching SmartDashboard
- ◆ Lab 3: Defining Basic Objects
- ◆ Detecting IP Spoofing
 - Configuring Anti-Spoofing
- ◆ Multicasting
 - Configuring Multicast Access Control
 - Interface Properties Multicast Restrictions
 - IGMP
 - Multicast Routing Protocols
 - Multicast Traffic
- ◆ Creating the Rule Base
 - Basic Rule Base Concepts
 - The Default Rule
 - Basic Rules
 - Implicit / Explicit Rules
 - Control Connections

- ◆ Completing the Rule Base
 - Understanding Rule Base Order
- ◆ Lab 4: Configuring Anti-Spoofing Measures
- ◆ Lab 5: Defining Basic Rules
- ◆ Security Policy Command-Line Options
 - cpstart
 - cpstop
 - fw Commands
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 4: Network Address Translation

- ◆ Objectives
- ◆ Key Terms
- ◆ Understanding Network Address Translation
 - IP Addressing
 - Dynamic NAT
 - Static NAT
- ◆ Configuring Network Address Translation
 - Global Properties
 - Dynamic NAT Object Configuration
 - Static NAT Object Configuration
- ◆ Manual NAT
 - When to Use Manual NAT
 - Configuring Manual NAT
 - Special Considerations
- ◆ Lab 6: Configuring Hide NAT
- ◆ Lab 7: Configuring Static NAT
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 5: Monitoring Traffic and Connections

- ◆ Objectives
- ◆ Key Terms
- ◆ SmartView Monitor
 - SmartView Monitor Login
 - Key Features
 - Monitoring Suspicious Activity Rules
 - Monitoring Alerts
 - Monitoring Gateways
 - Monitoring Traffic or Counters
 - Monitoring Tunnels
 - Monitoring Remote Users
- ◆ Lab 8: Setting Up Suspicious Activity Rule in SmartView Monitor
- ◆ Lab 9: Checking Status in SmartView Monitor
- ◆ Eventia Reporter
 - Eventia Reporter Login
 - Key Features
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 6: SmartDefense

- ◆ Objectives
- ◆ Key Terms
- ◆ Active Defense
 - Components of SmartDefense
 - SmartDefense Capabilities
- ◆ SmartDefense in Action
 - Anti-Spoofing Configuration Status
 - Denial-of-Service Attacks
 - IP and ICMP
 - TCP
 - Successive Events
 - Web Intelligence
 - Centralized Control Against Attacks
 - On-Line Updates
- ◆ Lab 10: Configuring SmartDefense
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 7: Content Security

- ◆ Objectives
- ◆ Key Terms
- ◆ Role of the Security Server
 - Security Server Overview
 - OPSEC
- ◆ Understanding Content Security
- ◆ Content Vectoring Protocol (CVP)
 - Inspection
- ◆ URI Filtering Protocol (UFP)
 - How UFP Works
- ◆ Implementing Content Security
 - Security Considerations
 - URI Filtering
 - Mail — SMTP
 - FTP Security Server
 - Blocking FTP over HTTP for Specific Groups
 - Java and ActiveX Stripping
 - CVP Inspection
- ◆ Resources and the Rule Base
 - Proper Rule Placement
 - Consequences of Incorrectly Configured Rules
- ◆ CVP Load Sharing and Chaining
 - CVP Chaining
- ◆ Implementing the TCP Resource
 - Configuring TCP Security Servers
 - TCP Resource Properties
 - UFP Tab
 - CVP Tab
- ◆ Lab 11: URL Screening by File
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 8: Authentication

- ◆ Key Terms
- ◆ Objectives
- ◆ Understanding Authentication
 - User Authentication
 - Session Authentication
 - Client Authentication
 - Authentication Types
 - Authentication Schemes
- ◆ User Authentication
- ◆ Client Authentication
 - How Client Authentication Works
 - Sign-on Methods
- ◆ Lab 12: Defining User Templates
- ◆ Lab 13: Defining Users
- ◆ Lab 14: Configuring User Authentication
- ◆ Lab 15: Setting Authentication Parameters (Optional)
- ◆ Lab 16: Configuring Client Authentication
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 9: LDAP User Management with SmartDirectory

- ◆ Objectives
- ◆ Key Terms
- ◆ LDAP Servers
 - Introduction to Account Management
 - Multiple LDAP Servers
- ◆ Integrating LDAP with NGX
 - Exporting Users
 - Using an Existing LDAP Server
- ◆ Using SmartDashboard to Manage LDAP Users
 - Organizational Units
 - Before Starting Account Management
 - Deleting an Object Tree
 - Defining Users

- ◆ LDAP and User Manager Troubleshooting
 - LDAP Issues
 - Schema Checking
 - User Manager Issues
 - NGX Issues
 - Important Debugging Tools
- ◆ Lab 17: Configuring LDAP Authentication with SmartDirectory
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 10: Configuring VPNs

- ◆ Objectives
- ◆ Key Terms
- ◆ IKE
 - Gateway-to-Gateway Configuration
 - Specifying Encryption
- ◆ VPN Deployments
 - Intranet VPNs
 - Remote-Access VPNs
- ◆ VPN Implementation
 - Three Critical VPN Components
- ◆ VPN Setup
 - Understanding VPN Deployment
- ◆ Simplified Intranet Setup
 - VPN Community Principles
- ◆ Integrating VPNs into a Rule Base
- ◆ Lab 18: Two-Gateway IKE Encryption Configuration (Shared Secret)
- ◆ Lab 19: Two-Gateway IKE Encryption Configuration (Certificates)
- ◆ Review
 - Review Questions
 - Review Answers

Chapter 11: Disaster Recovery

- ◆ Objectives
- ◆ Key Terms
- ◆ Backing Up for Disaster Recovery
 - \$FWDIR/conf
 - \$FWDIR/lib
 - fwauth.NDB
 - Exporting User Database Only
 - Backing Up Using ExportLab
- ◆ Lab 20: Backup and Restore
- ◆ Review
 - Review Questions
 - Review Answers