

Check Point Security Administration NGX I & II

(rev 1.1)



Course Code: NGX-I & II

Overview of NGX I

Check Point Security Administration NGX I Rev 1.1 is a foundation course for Check Point's flagship product, VPN-1 NGX. This course is intended to provide an understanding of basic concepts and skills necessary to configure VPN-1 NGX. During this course, students will configure a Security Policy, and learn about managing a firewalled network.

Pre-Requisites

Basic networking knowledge, knowledge of Windows Server and/or UNIX, and experience with TCP/IP and the Internet.

Who should take this class?

- You are a systems administrator, security manager, or network engineer who manages NGX Security Gateway deployments
- Want to earn Check Point Certified Security Administrator (CCSA NGX) NGX certification

What you will learn

- How VPN-1 NGX components and Check Point's Secure Virtual Network Architecture protect critical information assets
- How to create rules and modify a Security Policy's properties
- How to use advanced NGX features to minimize the information-security management burden, when working with objects and rules
- How to use monitoring tools to track, monitor, and account for all connections logged by Check Point components
- How to protect organizations from known network attacks and entire categories of emerging or unknown attacks, using SmartDefense
- How to use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations
- How to identify and address NGX security issues, including encryption and Virtual Private Networks
- How to verify the identity of users logging in to NGX, using NGX authentication schemes
- How to implement LDAP, and integrate it with NGX SmartCenter Server

- How to back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers

Exercises:

- Installing VPN-1 NGX in a stand-alone environment
- Launching SmartDashboard
- Defining basic objects
- Configuring anti-spoofing measures
- Defining basic rules
- Creating objects using object cloning
- Using Database Revision Control
- Blocking intruder connections
- Setting up a Suspicious Activity Rule in SmartView Monitor
- Checking status in SmartView Monitor
- Configuring SmartDefense
- Configuring Hide NAT
- Configuring Static NAT
- Encryption math and mechanics
- Defining user templates
- Defining users
- Configuring User Authentication
- Configuring Client Authentication
- Configuring LDAP authentication with SmartDirectory
- Backing up and restoring a Security Gateway and SmartCenter Server

Note: Table of Content available upon request (ngx1_toc.pdf)



REGISTRATION AND INFORMATION

education@ecs.com.sg

www.ecs.com.sg/training

TEL: (65) 6393-4737 (65) 6393-4741 (65) 6393-4743

FAX: (65) 6294-4097

ECS
佳杰科技

Page 1 of 2

Check Point Security Administration NGX I & II

(rev 1.1)



Course Code: NGX-I & II

Overview of NGX II

Check Point Security Administration NGX II is intended to provide an understanding of upgrading and advanced configuration of VPN-1 NGX, installing and managing VPN-1 NGX (on both internal and external networks), gaining the maximum security from Security Gateways, and resolving Security Gateway performance issues.

Pre-Requisites

Check Point Security Administration NGX I, or equivalent knowledge and experience

Who should take this class?

- You are a systems administrator, security manager, or network engineer implementing VPN-1 NGX for VPN deployments
- Want to earn Check Point Certified Security Expert ([CCSE NGX](#)) NGX certification

What you will learn

- How to use NGX tools to install VPN-1 NGX on Windows Server 2003 and SecurePlatform
- How to use NGX tools to upgrade to VPN-1 NGX, from VPN-1/FireWall-1 NG or VPN-1 NG with Application Intelligence
- How to distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports
- How to configure VPNs, using IKE encryption and Check Point's simplified VPN setup
- How to use VPN-1 SecuRemote/SecureClient to configure remote access
- How to configure VPN-1 NGX to allow VoIP traffic to pass through a corporate Security Gateway
- How to allocate bandwidth, given a variety of Check Point QoS configurations
- How to identify the features and limitations of Check Point High Availability solutions

Exercises:

- Upgrading NG with AI R55 to VPN-1 NGX
- Installing VPN-1 NGX in a distributed deployment
- Installing VPN-1 Power Gateway on SecurePlatform Pro
- Screening a URL by file
- Two-gateway IKE encryption configuration (using a shared secret)
- Two-gateway IKE encryption configuration (using Certificates)
- Configuring remote access in an IKE VPN
- Installing VPN-1 SecuRemote
- Using VPN-1 SecuRemote in an IKE VPN
- Implementing Office Mode
- Configuring a gateway for VoIP communications
- Configuring a Check Point QoS Policy
- Deploying Management High Availability
- Deploying New Mode High Availability
- Configuring Load Sharing Unicast (Pivot) mode

Note: Table of Content available upon request ([ngx2_toc.pdf](#))



REGISTRATION AND INFORMATION

education@ecs.com.sg

www.ecs.com.sg/training

TEL: (65) 6393-4737 (65) 6393-4741 (65) 6393-4743

FAX: (65) 6294-4097

ECS
佳杰科技

Page 2 of 2