

Basic Network Security for Small Businesses

Based on Check Point Safe@Office Security Appliances version 7.5
(1 day)

Course Description

Network security is no longer the concern of large enterprise only. It is a well-known fact that small businesses today are no less vulnerable to network attacks and have become an easy target for cyber-criminals. Check Point Software Technologies (www.checkpoint.com), the market leader in enterprise firewall and VPN solutions, has brought together the power of enterprise-level security, ease of implementation, and state-of-the-art patented NGX technology and architecture, to provide robust and scalable security solutions that fit the network security needs of small businesses. The Safe@Office 500 security appliances product family provides a cost-effective, unified threat management (UTM) security solution that is based on Check Point Embedded NGX technology.

The purpose of this course is to help network security professionals understand small business security requirements, needs, and challenges, and to teach them how to install and configure a Safe@Office-based security solution in small business network environment. All topics covered in this course are accompanied by hands-on lab exercises.

***Special offer:* Participants in this course will receive a fully functional demo Safe@Office 500W wireless security appliance (not for resale), and one year of subscription-based services upon product registration.**

Who Should Attend?

The course is intended for:

- ✓ Network and security pre-sale and post-sale support specialists
- ✓ ISPs and MSSPs sales and support experts
- ✓ Resellers, integrators, and technology consultants
- ✓ Check Point partners oriented towards small business network security solutions

Course Objectives

Upon completion of this course, participants will be able to:

- ✓ Understand small business network security threats and deployment challenges
- ✓ Understand the Check Point Embedded NGX network security solutions for small businesses
- ✓ Install and configure a Safe@Office security appliance within a network
- ✓ Set up a basic firewall security policies
- ✓ Understand provisioning of value-added, subscription-based services through a Service Center
- ✓ Configure content inspection policies (Antivirus, Web Filtering)
- ✓ Configure IPSec-based Remote Access and Site-to-Site VPNs
- ✓ Use basic troubleshooting tools



Prerequisites

Participants should meet the following requirements:

- ✓ Basic knowledge of networking and network topologies
- ✓ Basic knowledge of TCP/IP and other Internet technologies
- ✓ Previous knowledge of network security is an advantage

Course Layout

The following topics will be covered:

| Topic | Description |
|--|---|
| Small Business Network Security Risks and Deployment Challenges | <ul style="list-style-type: none"> • Understanding general network security requirements, threats, and trends • Network security and the small business • Overview of the Check Point Embedded NGX network security solution for small businesses |
| Getting Started with the Safe@Office 500 Appliance | <ul style="list-style-type: none"> • Getting familiar with the Safe@Office 500 hardware • Getting familiar with the configuration portal |
| Installing a Safe@Office 500 network security appliance | <ul style="list-style-type: none"> • Configuring physical ports • Setting up internal networks (LAN and DMZ networks) • Setting up the Internet connection • Working with multiple Internet connections (ISP backup and WAN load balancing) • Understanding the routing table |
| The Safe@Office 500 Firewall | <ul style="list-style-type: none"> • Understanding Check Point-patented Stateful Inspection technology • Understanding the Safe@Office firewall security rulebase • Protecting against application vulnerabilities with SmartDefense • Logging security events |
| Configuring subscription based services | <ul style="list-style-type: none"> • Overview of subscription based services • Connecting to a Service Center |
| Configuring content filtering policies | <ul style="list-style-type: none"> • Overview of the Vstream Gateway Antivirus • Configuring antivirus scanning policies • Understanding web site access policies • Configuring local Web Rules (Black/White URL lists) • Configuring the web filtering service (category based web filtering) |
| Virtual Private Networking | <ul style="list-style-type: none"> • Configuring Remote Access VPN • Configuring Site-to-Site VPN |