

---

# Course Objectives

## ***Chapter 1: Introduction to Endpoint Security***

- Using fundamental Endpoint Security architecture and concepts, confirm communication between the server and clients.
- Understand Endpoint Security communications, modes and views.
- Manage Catalogs and groups to organize Endpoint Security users into units.
- Understand Endpoint Security policy types and the major features for providing security through policy administration.
- Select your client and policy types, and your security model to plan a pilot installation before implementing in an enterprise environment.
- Considering recommended administrative workflow, install Check Point Endpoint Security Management Server on a Windows 2003 environment.

## ***Chapter 2: The Security Infrastructure***

- Understand Security Policy types, concepts, management strategies, and implementation.
- Configure firewall and program rules by selecting appropriate policy options in the Endpoint Security Management Server.
- Configure Zone-based security detection options, define Zones and set security levels based on user activity and network compliance criteria.
- Create and configure policies to deploy and assign to endpoints.

---

### ***Chapter 3: Advanced Features***

- Configure spyware and virus protection to customize options and perform scans.
- Enforce Endpoint Security using enforcement rules.
- Implement Endpoint Security High Availability using both local and standalone SmartCenter Servers.

### ***Chapter 4: Network Configuration and VPNs***

- Configure the client and server-side VPN connection.
- Create, deploy and test an endpoint VPN policy.



