
Course Objectives

Chapter 1: Check Point Technology Overview

- Describe Check Point's unified approach to network management, and the key elements of this architecture.
- Design a distributed environment using the network detailed in the course topology.
- Install the Security Gateway version R70 in a distributed environment using the network detailed in the course topology.

Chapter 2: Check Point Software Blades

- Given CheckPoint's latest integration of CoreXL technology, select the best security solution for your corporate environment.

Chapter 3: Deployment Platforms

- Given network specifications, perform a backup and restore the current Gateway installation from the command line.
- Identify critical files needed to purge or backup, import and export users and groups and add or delete administrators from the command line.
- Deploy Gateways using sysconfig and cpconfig from the Gateway command line.

Chapter 4: Introduction to the Security Policy

- Given the network topology, create and configure network, host and gateway objects.
- Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard.
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use.
- Configure NAT rules on Web and Gateway servers.
- Evaluate existing policies and optimize the rules based on current corporate requirements.
- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime.

Chapter 5: Monitoring Traffic and Connections

- Use queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data.
- Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, and ensure network functionality.
- Using SmartView Monitor, configure alerts and traffic counters, view a Gateway's status, monitor suspicious activity rules, analyze tunnel activity and monitor remote user access based on corporate requirements.

Chapter 6: Using SmartUpdate

- Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications.
- Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways.
- Upgrade and attach product licenses using SmartUpdate.

Chapter 7: Upgrading to R70

- Based on current products or platforms used in an enterprise network, perform a preinstallation compatibility assessment before upgrading to R70.
- Given R70 licensing restrictions, obtain a license key.
- Install a Contract File on platforms such as Windows, SecurePlatform, Linux, Solaris and IPSO.

Chapter 8: User Management and Authentication

- Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely.
- Manage users to access to the corporate LAN by using external databases.

Chapter 9: Encryption and VPNs

- Select the most appropriate encryption algorithm when securing communication over a VPN, based on corporate requirements.
- Establish VPN connections to partner sites in order to establish access to a central database by configuring Advanced IKE properties.

Chapter 10: Introduction to VPNs

- Configure a pre-shared secret site-to-site VPN with partner sites.
- Configure permanent tunnels for remote access to corporate resources.
- Configure VPN tunnel sharing, given the difference between host-based, subnet-based and gateway-based tunnels.

Chapter 11: Messaging and Content Security

- Configure Check Point Messaging Security to test IP Reputation, content based anti-spam, and zero hour virus detection.
- Based on network analysis disclosing threats by specific sites, configure a Web-filtering and antivirus policy to filter and scan traffic.

Chapter 12: Check Point IPS

- Implement default or customized profiles to designated Gateways in the corporate network.
- Manage profiles by tracking changes to the network, including performance degradation, and troubleshoot issues with the network related to specific IPS policy rules.
- Create and install IPS policies.