
Course Objectives

Chapter 1: Overview

- Given your understanding of Check Point's three-tier architecture and basic firewall concepts, design and install a distributed deployment of VPN-1.
- Test to verify the VPN-1 deployment, based on SIC establishment between the SmartCenter Server and the Gateway using SmartDashboard.

Chapter 2: Introduction to SecurePlatform

- Given the most current configuration, update the appropriate network interface using the sysconfig utility to change the management interface.
- Given specific instructions, perform a backup and restore of the current Gateway installation from the command line.

Chapter 3: Upgrading VPN-1

- Determine which VPN-1 upgrade strategy is appropriate, given a variety of scenarios.
- Determine VPN-1 license requirements, based on upgrade strategy.

Chapter 4: Introduction to the Security Policy

- Given the network topology, create and configure network, host, and gateway objects for your city site.
- In SmartMap view, actualize your city site's network objects.
- In SmartMap, given your partner city's network data, create and configure your partner city's Web server object.
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use. Test your Rule Base with your partner city, and evaluate logs in SmartView Tracker.
- Given your Policy's implicit rules, configure an implied rule for logging purposes.
- Manually configure NAT rules on your Web-server and Gateway objects. Refer to the Global Properties of the Gateway object.
- Configure the Policy using Database Revision Control.

Chapter 5: Monitoring Traffic and Connections

- Conduct and log daily network traffic.
- Identify potential holes or problems in the existing network structure.
- Address network-security concerns, i.e., suspicious activities, illegal services, blocked connections, etc.
- Perform rule sorting, to ensure each rule is properly matched or to delete obsolete rules that are never matched.
- Plan or adjust for proper network capacity.
- Ensure Policy compliance for Web surfing.
- Identify most- and-least visited pages on your company Web site for a proper sales and marketing perspective.

Chapter 6: Basic SmartDefense and Content Inspection

- Using content inspection, Application Intelligence, and/or Web Intelligence, configure for port scanning and HTTP worm catcher.
- Create a SmartDefense profile, and incorporate port-scanning and successive-events settings into the profile. Test the configuration with your partner city's Web server, and evaluate logs using SmartView Tracker.
- Block connections, given evidence of a potential intrusion or attack. Evaluate logs.
- Based on network analysis disclosing threats by specific sites, configure a Web-filtering and antivirus Policy to filter and/or scan the threatening traffic.

Chapter 7: Site to Site VPNs

- Select the appropriate VPN deployment to meet requirements, given a variety of scenarios.
- Configure VPN-1 to support site-to-site VPNs, given a variety of business requirements.
- Adjust VPN configuration settings to correct a problem, given symptoms of a configuration problem.

Chapter 8: Remote Access VPNs

- Configure VPN-1 to support remote-access VPNs, given a variety of business requirements.

Chapter 9: High Availability and ClusterXL

-
- Identify the features and limitations of Management High Availability.
 - Identify the benefits and limitations of different modes in a ClusterXL configuration.
 - Configure a ClusterXL VPN, given a specific business scenario.
 - Implement and test State Synchronization, given a business scenario.