Check Point Security Administration

Study Guide

CCSA
CHECK POINT CERTIFIED SECURITY ADMINISTRATOR

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.
Refer to the Third Party copyright notices (http:// www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

International Headquarters:	5 Ha'Solelim Street Tel Aviv 67897, Israel Tel: +972-3-753 4555
U.S. Headquarters:	959 Skyway Road, Suite 300 San Carlos, CA 94070 Tel: 650-628-2000 Fax: 650-654-4233
Technical Support, Education & Professional Services:	6330 Commerce Drive, Suite 120 Irving, TX 75063 Tel: 972-444-6612 Fax: 972-506-7913 E-mail any comments or questions about our courseware to courseware@us.checkpoint.com. For questions or comments about other Check Point documentation, e-mail CP_TechPub_Feedback@checkpoint.com.
Document #:	CPTS-DOC-CCSA-SG-R77

Preface

The Check Point Certified Security Administrator Exam

The *Check Point Security Administration* course provides an understanding of basic concepts and skills necessary to configure the Check Point Security Gateway, configure Security Policies, and learn about managing and monitoring secure networks.

The *Check Point Security Administration Study Guide* supplements knowledge you have gained from the Security Administration course, and is not a sole means of study.

The Check Point Certified Security Administrator #156-215.77 exam covers the following topics:

- 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 R77 in a distributed environment using the network detailed in the course topology.
- 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.
- 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.
- 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.
- Configure NAT rules on Web and Gateway servers.
- 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.
- 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.
- 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.
- Use Identity Awareness to provide granular level access to network resources.
- Acquire user information used by the Security Gateway to control access.
- Define Access Roles for use in an Identity Awareness rule.
- Implementing Identity Awareness in the Firewall Rule Base.

- 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, subunit-based and gateway-based tunnels.
- Resolve security administration issues.

Chapter 1: Introduction to Check Point Technology

Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This chapter introduces the basic concepts of network security and management based on Check Point's three-tier structure, and provides the foundation for technologies involved in the Check Point Software Blade Architecture, as discussed in the introduction. This course is lab-intensive, and in this chapter, you will begin your hands-on approach with a first-time installation using standalone and distributed topologies.

Objectives

- 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 in a distributed environment using the network detailed in the course topology.

Topics

The following table outlines the topics covered in the "Introduction to Check Point Technology" chapter of the *Check Point Security Administration Course.* This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topics	**Key Elements**
Check Point SecurityManagement Architecture(SMART)	
	SmartConsole Security Management Server Security Gateway
The Check Point Firewall	OSI Model Mechanism for controlling Network traffic. Packet Filtering Stateful Inspection Application Intelligence
Security Gateway Inspection Architecture	INSPECT Engine Packet Flow
DeploymentConsiderations	Standalone Deployment Distributed Deployment Standalone Full HA Bridge Mode
Check Point SmartConsole Clients	SmartDashboard Smartview Tracker SmartLog SmartEvent SmartView Monitor SmartReporter SmartUpdate SmartProvisioning SmartEndpoint
Security ManagementServer	Managing Users in SmartDashboard Users Database
Securing Channels of Communication	Secure Internal Communication Testing the SIC Status Resetting the Trust State

Lab 1: Distributed Installation	Install Security Management Server Configure Security Management Server - WebUI Configuring the Management Server Install Corporate Security Gateway Configure Corporate Security Gateway - WebUI Configuring the Corporate Security Gateway Installing SmartConsole
Lab 2: Branch Office Security Gateway Installation	Install SecurePlatform on Branch Gateway Configuring Branch Office Security Gateway with the First time Configuration Wizard Configure Branch Gateway - WebUI

Table 1-1: Introduction to Check Point Technology Topics

Sample Administrator Exam Question

The INSPECT engine inserts itself into the kernel between which two OSI model layers:

1. Physical and Data
2. Session and Transport
3. Data and Network.
4. Presentation and Application.

Answer

The INSPECT engine inserts itself into the kernel between which two OSI model layers:

1. Physical and Data
2. Session and Transport
3. **Data and Network.**
4. Presentation and Application.

Chapter 2: Deployment Platforms

Before delving into the intricacies of creating and managing Security Policies, it is beneficial to know about Check Point's different deployment platforms, and understand the basic workings of Check Point's Linux operating systems such as Gaia, that support many Check Point products - and what those products are.

Objectives:

- 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 from the Gateway command line.

Topics

The following table outlines the topics covered in the "Deployment Platforms" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
Check Point DeploymentPlatforms	Security Appliances Security Software Blades Remote Access Solutions
Check Point Gaia	History - Power of Two Gaia Benefits of Gaia Gaia Architecture Gaia System Information
Lab 3: CLI Tools	Working in Expert Mode Applying Useful Commands in CLISH Add and Delete Administrators via the CLI Perform Backup and Restore

Table 2-1: Deployment Platforms Topics

Sample CCSA Exam Question

Which command displays the installed Security Gateway version?

1. fw ver.
2. fw stat
3. fw printver
4. cpstat -gw

Answer

Which command displays the installed Security Gateway version?

1. **fw ver**.
2. fw stat
3. fw printver
4. cpstat -gw

Chapter 3: Introduction to the Security Policy

The Security Policy is essential in administrating security for your organization's network. This chapter examines how to create rules based on network objects, and modify a Security Policy's properties. In addition, this chapter will teach you how to apply Database Revision Control and Policy Package management, to decrease the burden of management when working with rules and objects.

Objectives:

- 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.
- 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.

Topics

The following table outlines the topics covered in the "Introduction to the Security Policy" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
Security Policy Basics	The Rule Base Managing Objects in SmartDashboard SmartDashboard and Objects Object-Tree Pane Objects-List Pane Object Types Rule Base Pane
Managing Objects	Classic View of the Objects Tree Group View of the Objects Tree
Creating the Rule Base	Basic Rule Base Concepts Delete Rule Basic Rules Implicit/Explicit Rules Control Connections Detecting IP Spoofing Configuring Anti-Spoofing
Rule Base Management	Understanding Rule Base Order Completing the Rule Base
Policy Management andRevision Control	Policy Package Management

	Database Revision Control Multicasting
Lab 4: Building a Security Policy	Create Security Gateway Object Create GUI Client Object Create Rules for Corporate Gateway Save the Policy Install the Policy Test the Corporate Policy Create the Remote Security Gateway Object Create a New Policy for the Branch Office Combine and Organize Security Policies
Lab 5: Configure the DMZ	Create DMZ Objects in SmartDashboard Create DMZ Access Rules Test the Policy

Sample CCSA Exam Question

Which of the following describes the default behavior of an R77 Gateway?

1. Traffic is filtered using controlled port scanning..
2. IP protocol types listed as secure are allowed by default, i.e. ICMP,
3. TCP, UDP sessions are inspected.
4. All traffic is expressly permitted via explicit rules.
5. Traffic not explicitly permitted is dropped.

Answer

Which of the following describes the default behavior of an R77 Gateway?

1. Traffic is filtered using controlled port scanning..
2. IP protocol types listed as secure are allowed by default, i.e. ICMP,
1. TCP, UDP sessions are inspected.
2. All traffic is expressly permitted via explicit rules.
3. **Traffic not explicitly permitted is dropped.**

Chapter 4: Monitoring Traffic and Connections

To manage your network effectively and to make informed decisions, you need to gather information on the network's traffic patterns.

Objectives:

- 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.

Topics

The following table outlines the topics covered in the "Introduction to Monitoring Traffic and Connections" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
SmartView Tracker	Log Types SmartView Tracker Tabs Action Icons Log-File Management Administrator Auditing Global Logging and Alerting Time Setting Blocking Connections
SmartView Monitor	Customized Views Gateway Status View Traffic View Tunnels View Remote Users View Cooperative Enforcement View
Monitoring Suspicious Activity Rules	Monitoring Alerts
Gateway Status	Overall Status Software Blade Status Displaying Gateway Information
SmartView Tracker vs.SmartView Monitor	
Lab 6: Monitoring with SmartView Tracker	Launch SmartView Tracker Track by Source and Destination Modify the Gateway to Active SmartView Monitor

Table 4-1: Monitoring Traffic and Connections Topics

Sample CCSA Exam Question

Which R77 SmartConsole tool would you use to verify the installed Security Policy on a Security Gateway?

1. SmartView Server
2. SmartView Tracker
3. None, SmartConsole applications only communicate with the
1. Security Management Server
4. SmartUpdate

Answer

Which R77 SmartConsole tool would you use to verify the installed Security Policy on a Security Gateway?

1. SmartView Server
2. **SmartView Tracker**
3. None, SmartConsole applications only communicate with the
5. Security Management Server
4. SmartUpdate

Chapter 5: Network Address Translation

In computer networking, network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device

Objectives:

- Configure NAT rules on Web and Gateway servers

Topics

The following table outlines the topics covered in the "Network Address Translation" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study

Topic	**Key Element**
Introduction to NAT	IP Addressing Hid NAT Choosing the Hide Address in Hide NAT Static NAT Original Packet Reply Packet NAT Global Properties Object Configuration - Hid NAT Hide NAT Using Another Interface Static NAT
Manual NAT	Configuring Manual NAT Special Considerations ARP
Lab 7: Configure NAT	Configure Static NAT on the DMZ Server Test the Static NAT Address Configure Hide NAT on the Corporate Network Test the Hide NAT Address Observe Hide NAT Traffic Using fw monitor Configure Wireshark Observe Traffic Observe Static NAT Traffic Using fw monitor

Table 5-1: Network Address Translation Topics

Sample CCSA Exam Question

In SmartDashboard, **Translate destination on client side** is checked in **Global Properties**. When Network Address Translation is used:

1. VLAN tagging cannot be defined for any hosts protected by the Gateway.
2. The Security Gateway's ARP file must be modified.
3. It is not necessary to add a static route to the Gateway's routing table.
4. It is necessary to add a static route to the Gateway's routing table.

Answer

In SmartDashboard, **Translate destination on client side** is checked in **Global Properties**. When Network Address Translation is used:

1. VLAN tagging cannot be defined for any hosts protected by the Gateway.
2. The Security Gateway's ARP file must be modified.
3. **It is not necessary to add a static route to the Gateway's routing table**.
4. It is necessary to add a static route to the Gateway's routing table.

Chapter 6: Using SmartUpdate

SmartUpdate extends your organization's ability to provide centralized policy management across enterprise-wide deployments. SmartUpdate can deliver automated software and license updates to hundreds of distributed Security Gateways from a single management console.

Objectives:

- 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.

Topics

The following table outlines the topics covered in the "Using SmartUpdate" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
SmartUpdate and Managing Licenses	SmartUpdate Architecture SmartUpdate Introduction Overview of Managing Licenses License Terminology Upgrading Licenses Retrieving License Data from Security Gateways Adding New Licenses to the License & Contract Repository Importing License Files Adding License Details Manually Attaching Licenses Detaching Licenses Deleting Licenses From License & Contract Repository Installation Process
Viewing License Properties	Checking for Expired Licenses To Export a License to a File
Service Contracts p.	Managing Contracts Updating Contracts

Table 6-6: Using SmartUpdate Topics

Sample CCSA Exam Question

What physical machine must have access to the User Center public IP address when checking for new packages with SmartUpdate?

1. SmartUpdate Repository SQL database Server.
2. A Security Gateway retrieving the new upgrade package.
3. SmartUpdate installed Security Management Server PC.
4. SmartUpdate GUI PC

Answer

What physical machine must have access to the User Center public IP address when checking for new packages with SmartUpdate?

1. SmartUpdate Repository SQL database Server.
2. A Security Gateway retrieving the new upgrade package.
3. SmartUpdate installed Security Management Server PC.
4. **SmartUpdate GUI PC**

Chapter 7: User Management and Authentication

If you do not have a user-management infrastructure in place, you can make a choice between managing the internal-user database or choosing to implement an LDAP server. If you have a large user count, Check Point recommends opting for an external user-management database, such as LDAP.

Check Point authentication features enable you to verify the identity of users logging in to the Security Gateway, but also allow you to control security by allowing some users access and disallowing others. Users authenticate by proving their identities, according to the scheme specified under a Gateway authentication scheme, such as LDAP, RADIUS, SecurID and TACACS.

Objectives:

- 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

Topics

The following table outlines the topics covered in the "User Management and Authentication" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
Creating Users and Groups	User Types
Security Gateway Authentication	Types of Legacy Authentication p. 142 Authentication Schemes p. 143 Remote User Authentication p. 145 Authentication Methods p. 146
User Authentication	User Authentication Rule Base Considerations
Session Authentication	Configuring Session Authentication
Client Authentication	Client Authentication and Sign-On Overview Sign-On Methods Wait Mode Configuring Authentication Tracking
LDAP User Management with UserDirectory	LDAP Features Distinguished Name Multiple LDAP Servers Using an Existing LDAP Server Configuring Entities to Work with the Gateway Defining an Account Unit Managing Users UserDirectory Groups
Lab 8: Configuring User Directory	Connect User Directory to Security Management Server

Table 7-1: User Management and Authentication Topics

Sample CCSA Exam Question

Which of the following are authentication methods that Security Gateway R77 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

1. User, Client, Session.
2. Proxied, User, Dynamic, Session.
3. Connection, User, Client.
4. User, Proxied, Session.

Answer

Which of the following are authentication methods that Security Gateway R77 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

1. **User, Client, Session.**
2. Proxied, User, Dynamic, Session.
3. Connection, User, Client.
4. User, Proxied, Session.

Chapter 8: Identity Awareness

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

Objectives:

- Use Identity Awareness to provide granular level access to network resources.
- Acquire user information used by the Security Gateway to control access.
- Define Access Roles for use in an Identity Awareness rule.
- Implementing Identity Awareness in the Firewall Rule Base.

Topics

The following table outlines the topics covered in the "Identity Awareness" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study.

Topic	**Key Element**
Introduction to Identity Awareness	AD Query Browser-Based Authentication Identity Agents Deployment
Lab 9: Identity Awareness	Configuring the Security Gateway Defining the User Access Role Applying User Access Roles to the Rule Base Testing Identity Based Awareness Prepare Rule Base for Next Lab

Table 8-1: Identity Awareness Topics

Sample CCSA Exam Question

What mechanism does a gateway configured with Identity Awareness and LDAP initially use to communicate with a Windows 2003 or 2008 server?

1. RCP
2. LDAP
3. WMI
4. CIFS

Answer

What mechanism does a gateway configured with Identity Awareness and LDAP initially use to communicate with a Windows 2003 or 2008 server?

1. RCP
2. LDAP
3. **WMI**
4. CIFS

Chapter 9: Introduction to Check Point VPNs

Virtual Private Networking technology leverages the Internet to build and enhance secure network connectivity. Based on standard Internet secure protocols, a VPN enables secure links between special types of network nodes: the Gateways. Site-to site VPN ensures secure links between Gateways. Remote Access VPN ensures secure links between Gateways and remote access clients.

Objectives:

- · 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.

Topics

The following table outlines the topics covered in the "Introduction to VPNs" chapter of the Check Point Security Administration Course. This table is intended as a supplement to knowledge you have gained from the Security Administration Courseware handbook, and is not meant to be a sole means of study

Topic	**Key Element**
The Check Point VPN	
VPN Deployments	Site-to-Site VPNs Remote-Access VPNs
VPN Implementation	VPN Setup Understanding VPN Deployment VPN Communities Remote Access Community
VPN Topologies	Meshed VPN Community Star VPN Community Choosing a Topology Combination VPNs Topology and Encryption Issues
Special VPN Gateway Conditions	Authentication Between Community Members Domain and Route-Based VPNs Domain-Based VPNs Route-Based VPN
Access Control and VPN Communities	Accepting All Encrypted Traffic Excluded Services Special Considerations for Planning a VPN Topology
Integrating VPNs into a Rule Base	Simplified vs. Traditional Mode VPNs VPN Tunnel Management Permanent Tunnels Tunnel Testing for Permanent Tunnels VPN Tunnel Sharing
Remote Access VPNs	Multiple Remote Access VPN Connectivity Modes Establishing a Connection Between a Remote User and a Gateway
Lab 10: Site-to-site VPN Between Corporate and Branch Office	Define the VPN Domain Create the VPN Community Create the VPN Rule and Modifying the Rule Base Test VPN Connection VPN Troubleshooting

Table 9-1: Introduction to VPNs

Sample CCSA Exam Question

What statement is true regarding Visitor Mode?

1. All VPN traffic is tunneled through UDP port 4500.
2. VPN authentication and encrypted traffic are tunneled through port TCP 433.
3. Only ESP traffic is tunneled through port TCP 443.
4. Only Main mode and Quick mode traffic are tunneled on TCP port 443.

Answer

What statement is true regarding Visitor Mode?

1. All VPN traffic is tunneled through UDP port 4500.
2. **VPN authentication and encrypted traffic are tunneled through port TCP 433.**
3. Only ESP traffic is tunneled through port TCP 443.
4. Only Main mode and Quick mode traffic are tunneled on TCP port 443.