Check Point™
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Security Administration Study Guide

R76 Edition

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-R76

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.xx 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 R76 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.

Frequently Asked Questions

The table below provides answers to commonly asked questions about the Check Point CCSA #156-315.xx exams:

Question	Answer
What are the Check Point recommendations and prerequisites?	Check Point recommends you have at least 6 months to 1 year of experience with the products, before attempting to take the CCSA # 156-215.xx exam. In addition, you should also have basic networking knowledge, knowledge of Windows Server and/or UNIX, and experience with TCP/IP and the Internet. Check Point also recommends you take the *Check Point Security Administration* class from a Check Point Authorized Training Center (ATC). We recommend you take this class before taking the CCSA # 156-215.xx exam. ***Check Point ATCs also offer Check Point's comprehensive #156-215.xx Exam Prep course (only available at Check Point ATCs).*** To locate an ATC, see: **`http://atc.checkpoint.com/atclocator/locateATC`**
How do I register?	Check Point exams are offered through Pearson VUE, a third-party testing vendor with more than 3,500 testing centers worldwide. Pearson VUE offers a variety of registration options. Register via the Web or visit a specific testing center. Registrations at a testing center may be made in advance or on the day you wish to test, subject to availability. For same-day testing, contact the testing center directly. Locate a testing center from the VUE Pearson Web site: **`www.pearsonvue.com`**

Question	Answer
What is the exam structure?	The exams are composed of multiple-choice and scenario questions. There is no partial credit for incorrectly marked questions.
How long is the exam? Do I get extra time, if I am not a native English speaker?	The following countries are given 90 minutes to complete the exam. All other regions get 120 minutes: Australia Bermuda Canada Japan New Zealand Ireland South Africa UK US
What are the pre-requisites for the CCSE R76 exam?	CCSA R70,CCSA 71, CCSA R75, or CCSA R76.
How can I update my R65 certification?	If you have any CCSA R60 certification, take the CCSA R70/71 Update Training Blade to update your CCSA certification. If you have a CCSE R60 certification, take the CCSE R70/71 Update Training Blade to update your CCSE certification.
How long is my certification valid?	Check Point certifications are valid for 2 years. CCMAs are valid for 3 years. Any certification more than three (3) years old is not considered current. Certifications become inactive after five years. Your benefits may be suspended if your certification is not current. Your certification can be maintained with annual continuing education credits.

Question	Answer
What are 'continuing education credits'?	Continuing education credits help you maintain Check Point certifications without starting over with every product release. Continuing education credits can be earned in a variety of ways like completing shorter training lessons (Training Blades), by participating in our test development process, and even attending CPX.
What are the pre-requisites for CCMA?	CCSE is mandatory; CCMSE is suggested.
Do you have a test-out option?	Though highly recommended, it is not a requirement to attend a training course before challenging the exam. You may test at any time, however it is advised you spend at least 6 months working with Check Point products before attempting to achieve certification.
Are study materials available?	Free study guides and practice exams are available for download at **http://www.checkpoint.com/services/education/index.html#resources.** Courseware can be purchased on our eStore and Training is available from an ATC. ***Check Point ATCs also offer Check Point's comprehensive #156-215.xx Exam Prep course (only available at Check Point ATCs).***
How soon can I re-take an exam if I fail?	If you fail an exam you must wait 24 hours before your 2nd attempt, and 30 days for the 3rd attempt. Once you pass a test you cannot take it again for a higher score.
Can I get exam insurance?	Students automatically get a 50% re-take discount on any 2nd attempt of the CCSA and CCSE R76 exams.

Question	Answer
I only failed by 1 point and based on my calculations I should have passed – what happened?	The function of certification is to provide proof the Check Point Certified professional is qualified to protect the lifeblood of organizations – their data. Check Point takes this very seriously and we constantly strive to administer the most effective exams. Passing is calculated by comparing the number of questions answered correctly versus the number of questions answered incorrectly. Not all sections of the test are weighted equally.
Can I take any R65 level exams?	No, all R65 exams have been retired except for the Japanese versions. Our philosophy is to provide training and certification only for current technologies so our partners and customers will always benefit from the latest security advancements.
Where can I find more information about Check Point Certified Professionals?	The Check Point Certified Professionals website and newsletter are a benefit which contain special information and resources that are not available to the public.
What happens when I pass my exam? When will I receive my Certificate?	After you pass a Check Point exam at VUE, your exam results are uploaded. On the 15th and 30th, we process all certification results and order certification kits. It takes 6-8 weeks to receive your certificate. Your advanced access to Secure Knowledge and the Certified Professionals website is established once you achieve certification.
Why can't I have more than one account at Pearson VUE test centers?	Check Point only allows one Pearson VUE account to track your Check Point exams. If you change companies, please update the contact information in your Pearson VUE account instead of creating a new one so your Check Point certifications will follow you. You can verify your accounts with Customer Service here: **http://www.vue.com/checkpoint/contact/**

Question	Answer
What happens if someone gets caught cheating? How do you prevent it?	Every individual who takes an exam signs our Non-disclosure agreement. Anyone caught in the act of cheating or sharing exam items will have their Check Point certifications revoked for 2 years. All testing privileges and partner program participation will be deactivated during this time. Check Point collaborates with major technology companies to prevent cheating through test pattern analysis and distribution best practices. Together we identify and take legal action against unauthorized test centers and inaccurate "brain dump" sites.
What are the benefits of Check Point certification?	Check Point Certified Professionals receive access to the Advanced SecureKnowledge base, Certified Professionals only website and quarterly newsletter for 2 years. Check Point Certified Master Architects (CCMA) receive 3 years Expert level access to SecureKnowledge.
How do take a Training Blade exam?	You can purchase Training Blades at http://store.checkpoint.com. Please forward your email confirmation to: **examcentral@checkpoint.com** for access to the exam. Please include your Check Point Certified Professional ID# for credit. Your certification ID# is generated when you create an account at Pearson VUE. If you have any questions about your ID#, please email: **accountservices@checkpoint.com**.
How do I access my certification benefits?	Make sure your Check Point User Center (UC) email address matches the email address registered with Pearson VUE. Your UC profile will automatically be updated with each certification, including advanced access to SecureKnowledge and the Certified Professionals only website. If you have any problems or questions about your benefits please email: **certification@checkpoint.com**

For more exam and course information, see:

http://www.checkpoint.com/services/education/

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.

Introduction to Check Point Technology 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	Page Numbers
Check Point Security Management Architecture (SMART)		p. 09
	SmartConsole Security Management Server Security Gateway	p. 10
The Check Point Firewall		p. 11
	OSI Model Mechanism for controlling Network traffic. Packet Filtering Stateful Inspection Application Intelligence	p. 11 p. 12 p. 13 p.14 p. 15
Security Gateway Inspection Architecture		p. 8
	INSPECT Engine Packet Flow	p. 16
Deployment Considerations		p. 18

Table 1-1: Introduction to Check Point Technology Topics

Topics	Key Elements	Page Numbers
	Standalone Deployment	p. 19
	Distributed Deployment	p. 19
	Standalone Full HA	p. 20
	Bridge Mode	p. 20
Check Point SmartConsole Clients		p. 21
	SmartDashboard	p. 21
	Smartview Tracker	p. 23
	SmartLog	p. 24
	SmartEvent	p. 24
	SmartView Monitor	p. 26
	SmartReporter	p. 27
	SmartUpdate	p. 28
	SmartProvisioning	p. 29
	SmartEndpoint	p. 31
Security Management Server		p. 32
	Managing Users in SmartDash-board	p. 32
	Users Database	p. 33
Securing Channels of Communication		p.34
	Secure Internal Communication	p. 34
	Testing the SIC Status	p. 35
	Resetting the Trust State	p. 36

Table 1-1: Introduction to Check Point Technology Topics

Topic	Key Element	Page Number
Lab 1: Distributed Installation		L-p. 5
	Install Security Management Server	L-p. 16
	Configure Security Management Server - Web UI	L-p. 12
	Configuring the Management Server	L-p. 28
	Install Corporate Security Gateway	L-p. 30
	Configure Corporate Security Gateway - WebUI	L-p. 37
	Configuring the Corporate Security Gateway	L-p. 46
	Installing SmartConsole	L-p. 54
Lab 2: Branch Office Security Gateway Installation		L-p. 61
	Install SecurePlatform on Branch Gateway	L-p. 62
	Configuring Branch Office Security Gateway with the First time Configuration Wizard	L-p. 68
	Configure Branch Gateway - WebUI	L-p. 76

Table 1-2: Check Point Technology Overview - Lab Topics

Sample CCSA 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.

Deployment Platforms 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	Page Number
Check Point Deployment Platforms		p. 41
	Security Appliances	p. 41
	Security Software Blades	p. 46
	Remote Access Solutions	p. 48
Check Point Gaia		p. 50
	History - Power of Two	p. 50
	Gaia	p. 52
	Benefits of Gaia	p. 52
	Gaia Architecture	p. 53
	Gaia System Information	p. 58

Table 2-1: Deployment Platforms Topics

Topic	Key Element	Page Number
Lab 3: CLI Tools		L-p. 87
	Working in Expert Mode	L-p. 88

Table 2-2: Deployment Platform- Lab Topics

Topic	Key Element	Page Number
	Applying Useful Commands in CLISH	L-p. 92
	Add and Delete Administrators via the CLI	L-p. 94
	Perform Backup and Restore	L-p. 96

Table 2-2: Deployment Platform- Lab 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.

Introduction to the Security Policy 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**	**Page Number**
Security Policy Basics		p. 63
	The Rule Base	p. 63
	Managing Objects in SmartDashboard	p. 63
	SmartDashboard and Objects	p. 64
	Object-Tree Pane	p. 64
	Objects-List Pane	p. 65
	Object Types	p. 65
	Rule Base Pane	p. 65
Managing Objects		p. 66
	Classic View of the Objects Tree	p. 67
	Group View of the Objects Tree	p. 67
Creating the Rule Base		p. 68
	Basic Rule Base Concepts	p. 68
	Delete Rule	p. 69\p.
	Basic Rules	p. 70
	Implicit/Explicit Rules	p. 71
	Control Connections	p. 71
	Detecting IP Spoofing	p. 72
	Configuring Anti-Spoofing	p. 73
Rule Base Management		p. 74

Table 3-1: Security Policy Topics

Topic	Key Element	Page Number
	Understanding Rule Base Order	p. 75
	Completing the Rule Base	p. 76
Policy Management and Revision Control		p. 77
	Policy Package Management	p. 77
	Database Revision Control	p. 78
	Multicasting	p. 80

Table 3-1: Security Policy Topics

Topic	Key Element	Page Number
Lab 4: Building a Security Policy		L-p. 99
	Create Security Gateway Object	L-p. 100
	Create GUI Client Object	L-p. 111
	Create Rules for Corporate Gateway	L-p. 113
	Save the Policy	L-p. 119
	Install the Policy	L-p. 120
	Test the Corporate Policy	L-p. 123
	Create the Remote Security Gateway Object	L-p. 124
	Create a New Policy for the Branch Office	L-p. 131
	Combine and Organize Security Policies	L-p. 136

Table 3-2: Security Policy - Lab Topics

Topic	Key Element	Page Number
Lab 5: Configure the DMZ		L-p. 147
	Create DMZ Objects in SmartDashboard	L-p. 148
	Create DMZ Access Rules	L-p. 150
	Test the Policy	L-p. 151

Table 3-2: Security Policy - Lab Topics

Sample CCSA Exam Question

Which of the following describes the default behavior of an R76 Gateway?

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

Answer

Which of the following describes the default behavior of an R76 Gateway?

1. Traffic is filtered using controlled port scanning..
2. IP protocol types listed as secure are allowed by default, i.e. ICMP, TCP, UDP sessions are inspected.
3. All traffic is expressly permitted via explicit rules.
4. **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.

Introduction to the Monitoring Traffic and Connections 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	Page Number
SmartView Tracker		p. 84
	Log Types	p. 85
	SmartView Tracker Tabs	p. 87
	Action Icons	p. 88
	Log-File Management	p. 89
	Administrator Auditing	p. 89
	Global Logging and Alerting	p. 90
	Time Setting	p. 91
	Blocking Connections	p. 92
SmartView Monitor		p. 94
	Customized Views	p. 95
	Gateway Status View	p. 95
	Traffic View	p. 95
	Tunnels View	p. 96
	Remote Users View	p. 97
	Cooperative Enforcement View	p. 98
Monitoring Suspicious Activity Rules		p. 99
	Monitoring Alerts	p. 100
Gateway Status		p. 102

Table 4-1: Monitoring Traffic and Connections Topics

Topic	Key Element	Page Number
	Overall Status Software Blade Status Displaying Gateway Information	p. 103 p. 104 p.104
SmartView Tracker vs. SmartView Monitor		p. 105

Table 4-1: Monitoring Traffic and Connections Topics

Topic	Key Element	Page Number
Lab 6: Monitoring with SmartView Tracker		L-p. 153
	Launch SmartView Tracker Track by Source and Destination Modify the Gateway to Active SmartView Monitor	L-p. 154 L-p. 155 L-p. 158

Table 4-2: Monitoring Traffic and Connections - Lab Topics

Sample CCSA Exam Question

Which R76 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 Security Management Server
4. SmartUpdate

Answer

Which R76 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 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

Network Address Translation 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**	**Page Number**
Introduction to NAT		p. 109
	IP Addressing	p. 110
	Hid NAT	p. 110
	Choosing the Hide Address in Hid NAT	p. 111
	Static NAT	p. 111
	Original Packet	p. 112
	Reply Packet	p. 112
	NAT Global Properties	p. 113
	Object Configuration - Hid NAT	p. 114
	Hide NAT Using Another Interface	p. 116
	Static NAT	p. 117
Manual NAT		p. 118
	Configuring Manual NAT	p. 118
	Special Considerations	p. 119
	ARP	p. 119

Table 5-1: Network Address Translation Topics

Topic	Key Element	Page Number
Lab 7: Configure NAT		L-p. 165
	Configure Static NAT on the DMZ Server	L-p. 166
	Test the Static NAT Address	L-p. 168
	Configure Hide NAT on the Corporate Network	L-p. 169
	Test the Hide NAT Address	L-p. 173
	Observe Hide NAT Traffic Using fw monitor	L-p. 175
	Configure Wireshark	L-p. 178
	Observe Traffic	L-p 180
	Observe Static NAT Traffic Using fw monitor	L-p. 181

Table 5-2: Network Address Translation - Lab 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.

Using SmartUpdate Topics

The following table outlines the topics covered in the "IUsing 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	Page Number
SmartUpdate and Managing Licenses		p. 123
	SmartUpdate Architecture	p. 124
	SmartUpdate Introduction	p. 126
	Overview of Managing Licenses	p. 128
	License Terminology	p. 129
	Upgrading Licenses	p. 131
	Retrieving License Data from Security Gateways	p. 131
	Adding New Licenses to the License & Contract Repository	p. 131
	Importing License Files	p. 132
	Adding License Details Manually	p. 132
	Attaching Licenses	p. 133
	Detaching Licenses	p. 133
	Deleting Licenses From License & Contract Repository	p. 133
	Installation Process	p. 133
Viewing License Properties		p. 134
	Checking for Expired Licenses	p. 134

Table 6-6: Using SmartUpdate Topics

Topic	Key Element	Page Number
	To Export a License to a File	p. 134
Service Contracts		p. 135
	Managing Contracts Updating Contracts	p. 135 p. 136

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

Introduction to the User Management and Authentication 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	Page Number
Creating Users and Groups		p. 141
	User Types	p. 141
Security Gateway Authentication		p. 142
	Types of Legacy Authentication	p. 142
	Authentication Schemes	p. 143
	Remote User Authentication	p. 145
	Authentication Methods	p. 146
User Authentication (Legacy		p. 148
	User Authentication Rule Base Considerations	p. 148
Session Authentication (Legacy)		p. 149
	Configuring Session Authentication	p. 151
Client Authentication (Legacy)		p. 152
	Client Authentication and Sign-On Overview	p. 152

Table 7-1: User Management and Authentication Topics

Topic	Key Element	Page Number
	Sign-On Methods	p. 153
	Wait Mode	p. 153
	Configuring Authentication Tracking	p. 154
LDAP User Management with UserDirectory		p. 156
	LDAP Features	p. 156
	Distinguished Name	p. 157
	Multiple LDAP Servers	p. 158
	Using an Existing LDAP Server	p. 158
	Configuring Entities to Work with the Gateway	p. 159
	Defining an Account Unit	p. 160
	Managing Users	p. 161
	UserDirectory Groups	p. 162

Table 7-1: User Management and Authentication Topics

Topic	Key Element	Page Number
Lab 8: Configuring User Directory		L-p. 187
	Connect User Directory to Security Management Server	L-p. 188
	Verify SmartDashboard Integration	L-p. 199

Table 7-2: User Management and Authentication - Lab Topics

Sample CCSA Exam Question

Which of the following are authentication methods that Security Gateway R76 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 R76 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.

Identity Awareness 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**	**Page Number**
Introduction to Identity Awareness		p. 167
	AD Query	p. 168
	Browser-Based Authentication	p. 173
	Identity Agents	p. 180
	Deployment	p. 186

Table 8-1: Identity Awareness Topics

Topic	**Key Element**	**Page Number**
Lab 9: Identity Awareness		L-p. 203
	Configuring the Security Gateway	L-p. 204
	Defining the User Access Role	L-p. 210
	Applying User Access Roles to the Rule Base	L-p. 214
	Testing Identity Based Awareness	L-p. 217
	Prepare Rule Base for Next Lab	L-p. 219

Table 8-2: Identity Awareness - Lab 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.

Introduction to VPNs 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	Page Number
The Check Point VPN		p. 191
VPN Deployments		p. 192
	Site-to-Site VPNs	p. 192
	Remote-Access VPNs	p. 193
VPN Implementation		p. 194
	VPN Setup	p. 195
	Understanding VPN Deployment	p. 195
	VPN Communities	p. 195
	Remote Access Community	p. 197
VPN Topologies		p. 198
	Meshed VPN Community	p. 198
	Star VPN Community	p. 199
	Choosing a Topology	p. 199
	Combination VPNs	p. 200
	Topology and Encryption Issues	p. 201
Special VPN Gateway Conditions		p. 202
	Authentication Between Community Members	p. 203
	Domain and Route-Based VPNs	p. 204

Table 9-1: Introduction to VPNs Topics

Topic	Key Element	Page Number
	Domain-Based VPNs	p. 204
	Route-Based VPN	p. 204
Access Control and VPN Communities		p. 205
	Accepting All Encrypted Traffic	p. 206
	Excluded Services	p. 207
	Special Considerations for Planning a VPN Topology	p. 207
Integrating VPNs into a Rule Base		p. 208
	Simplified vs. Traditional Mode VPNs	p. 209
	VPN Tunnel Management	p. 209
	Permanent Tunnels	p. 209
	Tunnel Testing for Permanent Tunnels	p. 210
	VPN Tunnel Sharing	p. 211
Remote Access VPNs		p. 213
	Multiple Remote Access VPN Connectivity Modes	p. 214
	Establishing a Connection Between a Remote User and a Gateway	p. 214

Table 9-1: Introduction to VPNs Topics

Topic	Key Element	Page Number
Lab 10: Site-to-site VPN Between Corporate and Branch Office		L-p. 221
	Define the VPN Domain	L-p. 222
	Create the VPN Community	L-p. 225
	Create the VPN Rule and Modifying the Rule Base	L-p. 233
	Test VPN Connection	L-p. 236
	VPN Troubleshooting	L-p. 241

Table 9-2: Introduction to VPNs - Lab Topics

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.