Check Point Security Engineering

Study Guide

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 Engineering Exam

The *Check Point Security Engineering* course provides an understanding of upgrading and advanced configuration of Check Point software blades, installing and managing VPNs (on both internal and external networks), gaining the maximum security from Security Gateways, and resolving Gateway performance issues.

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

The Check Point Certified Security Engineering #156-315.13 exam covers the following topics:

- The process for backup of a Security Gateway and Management Server using your understanding of the differences between backups, snapshots, and upgrade-exports.
- The process for upgrade of Management Server using a database migration.
- How to perform debugs on firewall processes.
- Building, testing and troubleshooting a ClusterXL Load Sharing deployment on an enterprise network.
- Building, testing and troubleshooting a ClusterXL High Availability deployment on an enterprise network.
- Building, testing and troubleshooting a management HA deployment on an enterprise network.
- Configuring, maintaining and troubleshooting SecureXL and CoreXL acceleration solutions on the corporate network traffic to ensure noted performance enhancement on the firewall.
- Building, testing and troubleshooting a VRRP deployment on an enterprise network.
- Using an external user database such as LDAP, to configure User Directory to incorporate user information for authentication services on the network.
- Managing internal and external user access to resources for Remote Access or across a VPN.
- Troubleshooting a site-to-site or certificate-based VPN on a corporate gateway using IKEView, VPN log files and command-line debug tools.
- Optimizing VPN performance and availability using Link Selection and Multiple Entry Point solutions.
- Managing and testing corporate VPN tunnels to allow for greater monitoring and scalability with multiple tunnels defined in a community including other VPN providers.
- Creating Events and using existing event definitions to generate reports on specific network traffic using SmartReporter and SmartEvent in order to provide industry compliance information to management.
- Troubleshoot report generation given command-line tools and debug-file information.

Chapter 1: Upgrading

Upgrades are used to save Check Point product configurations, Security Policies, and objects, so that Security Administrators do not need to re-create Gateway and Security Management Server configurations.

Objectives:

- Perform a backup of a Security Gateway and Management Server using your
- Understanding of the differences between backups, snapshots, and upgrade-exports.
- Upgrade and troubleshoot a Management Server using a database migration.
- Upgrade and troubleshoot a clustered Security Gateway deployment.

Topics

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

Topics	**Key Elements**
Backup and Restore Security Gateways and Management Servers	Snapshot management Upgrade Tools Backup Schedule Recommendations Upgrade Tools Performing Upgrades Support Contract
Upgrading Standalone Full High Availability	
Lab 1: Upgrading to Check Point R77	Install Security Management Server Migrating Management server Data Importing the Check Point Database Launch SmartDashboard Upgrading the Security Gateway

Table 1-1: Upgrade Topics

Sample CCSE Exam Question

During an upgrade to the management server, the contract file is transferred to a gateway when the gateway is upgraded. Where is the contract file retrieved from:

1) ISO
2) Technical Support
3) Management.
4) User Center.

Answer

During an upgrade to the management server, the contract file is transferred to a gateway when the gateway is upgraded. Where is the contract file retrieved from:

1) ISO
2) Technical Support
3) Management.
4) User Center.

Chapter 2: Advanced Firewall

The Check Point Firewall Software Blade builds on the award-winning technology, first offered in Check Point's firewall solution, to provide the industry's best gateway security with identity awareness. Check Point's firewalls are trusted by 100% of Fortune 100 companies and deployed by over 170,000 customers. Check Point products have demonstrated industry leadership and continued innovation since the introduction of FireWall-1 in 1994.

Objectives:

- Using knowledge of Security Gateway infrastructure, including chain modules, packet flow and kernel tables to describe how to perform debugs on firewall processes.

Topics

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

Topic	**Key Element**
Check Point Firewall Infrastructure	GUI Clients Management
Security Gateway	User and Kernel Mode Processes CPC Core Process FWM FWD CPWD Inbound and Outbound Packet Flow Inbound FW CTL Chain Modules Outbound Chain Modules Columns in a Chain Stateful Inspection
Kernel Tables	Connections Table Connections Table Format
Check Point Firewall Key Features	Packet Inspection Flow Policy Installation Flow Policy Installation Process Policy Installation Process Flow
Network Address Translation	How NAT Works Hide NAT Process Security Servers How a Security Server Works Basic Firewall Administration Common Commands
FW Monitor	What is FW Monitor C2S Connections and S2C Packets fw monitor
Lab 2: Core CLI Elements of Firewall Administration	Policy Management and Status Verification from the CLI Using cpinfo Run cpinfo on the Security Management Server Analyzing cpinfo in InfoView Using fw ctl pstat Using tcpdump

Table 2-1: Advanced Firewall Topics

Sample CCSE Exam Question

User definitions are stored in ___________________

1. $FWDIR/conf/fwmuser.conf
2. $FWDIR/conf/users/NDB
3. $FWDIR/conf/fwauth.NDB
4. $FWDIR/conf/conf/fwusers.conf

Answer

User definitions are stored in ___________________

1. $FWDIR/conf/fwmuser.conf
2. $FWDIR/conf/users/NDB
3. **$FWDIR/conf/fwauth.NDB**
4. $FWDIR/conf/conf/fwusers.conf

Chapter 3: Clustering and Acceleration

Whether your preferred network redundancy protocol is Check Point ClusterXL technology or standard VRRP protocol, it is no longer a “platform choice” you will have to make with Gaia. Both ClusterXL and VRRP are fully supported by Gaia, and Gaia is available to all Check Point Appliances, open servers and virtualized environments. There are no more trade-off decisions between required network protocols and preferred security platforms/functions.

Objectives:

- Build, test and troubleshoot a ClusterXL Load Sharing deployment on an enterprise network.
- Build, test and troubleshoot a ClusterXL High Availability deployment on an enterprise network.
- Build, test and troubleshoot a management HA deployment on an enterprise network.
- Configure, maintain and troubleshoot SecureXL and CoreXL acceleration solutions on the corporate network traffic to ensure noted performance enhancement on the firewall.
- Build, test and troubleshoot a VRRP deployment on an enterprise network.

Topics

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

Topic	**Key Element**
VRRP	VRRP vs ClusterXL Monitored Circuit VRRP Troubleshooting VRRP
Clustering and Acceleration	Clustering Terms ClusterXL Cluster Synchronization Synchronized-Cluster Restrictions Securing the Sync Interface To Synchronize or Not to Synchronize
ClusterXL: Load Sharing	Multicast Load Sharing Unicast Load Sharing How Packets Travel Through a Unicast LS Cluster Sticky Connections
Maintenance Tasks and Tools	Perform a Manual Failover of the FW Cluster Advanced Cluster Configuration
Management HA	The Management High Availability Environment Active vs. Standby What Data is Backed Up? Synchronization Modes Synchronization Status
SecureXL: Security Acceleration	What SecureXL Does Packet Acceleration Session Rate Acceleration Masking the Source Port Application Layer Protocol - An

	Example with HTTP HTTP 1.1 Factors that Preclude Acceleration Factors that Preclude Templating (Session Acceleration) Packet Flow VPN Capabilities
CoreXL: Multicore Acceleration	Supported Platforms and Features Default Configuration Processing Core Allocation Allocating Processing Cores Adding Processing Cores to the Hardware Allocating an Additional Core to the SND Allocating a Core for Heavy Logging Packet Flows with SecureXL Enabled
Lab 3 Migrating to a Clustering Solution	Installing and Configuring the Secondary Security Gateway Re-configuring the Primary Gateway Configuring Management Server Routing Configuring the Cluster Object Testing High Availability Installing the Secondary Management Server Configuring Management High Availability

Table 3-1: Clustering and Acceleration Topics

Sample CCSE Exam Question

A zero downtime upgrade of a cluster:

1. Upgrades all cluster members except one at the same time
2. Is only supported in major releases (R70,to R71, R71 to R77)
3. Treats each individual cluster member as an individual gateway
4. Requires breaking the cluster and upgrading members independently.

Answer

A zero downtime upgrade of a cluster:

1. **Upgrades all cluster members except one at the same time**
2. Is only supported in major releases (R70,to R71, R71 to R77)
3. Treats each individual cluster member as an individual gateway
4. Requires breaking the cluster and upgrading members independently.

Chapter 4: Advanced User Management

Consistent user information is critical for proper security. Without a centralized data store, managing user information across multiple applications can be a manual, error-prone process.

Objectives:

- Using an external user database such as LDAP, configure User Directory to incorporate user information for authentication services on the network.
- Manage internal and external user access to resources for Remote Access or across a VPN.
- Troubleshoot user access issues found when implementing Identity Awareness.

Topics

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

Topic	**Key Element**
User Management	Active Directory OU Structure Using LDAP Servers with Check Point LDAP User Management with User Directory Defining an Account Unit Configuring Active Directory Schemas Multiple User Directory (LDAP) Servers Authentication Process Flow Limitations of Authentication Flow User Directory (LDAP) Profiles
Troubleshooting User Authentication and User Directory (LDAP)	Common Configuration Pitfalls Some LDAP Tools Troubleshooting User Authentication
Identity Awareness	Enabling AD Query AD Query Setup Identifying users behind an HTTP Proxy Verifying there’s a logged on AD user at the source IP Checking the source computer OS Using SmartView Tracker
Lab 4: Configuring SmartDashboard to Interface with Active Directory	Creating the Active Directory Object in SmartDashboard Verify SmartDashboard Communication with the AD Server

Table 4-1: Advanced User Management Topics

Sample CCSE Exam Question

Choose the BEST sequence for configuring user managemetn in SmartDashboard, using an LDAP server.

1. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
2. Configure a server object for the LDAP Account Unit, and create an LDAP resource object

3. Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.
4. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

Answer

Choose the BEST sequence for configuring user managemetn in SmartDashboard, using an LDAP server.

1. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
2. Configure a server object for the LDAP Account Unit, and create an LDAP resource object
3. **Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.**
4. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

Chapter 5: Advanced IPsec VPN and Remote Access

Check Point's VPN Software Blade is an integrated software solution that provides secure connectivity to corporate networks, remote and mobile users, branch offices and business partners. The blade integrates access control, authentication and encryption to guarantee the security of network connections over the public Internet.

Objectives:

- Using your knowledge of fundamental VPN tunnel concepts, troubleshoot a site-to-site or certificate-based VPN on a corporate gateway using IKEView, VPN log files and command-line debug tools.
- Optimize VPN performance and availability by using Link Selection and Multiple Entry Point solutions.
- Manage and test corporate VPN tunnels to allow for greater monitoring and scalability with multiple tunnels defined in a community including other VPN providers.

Topics:

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

Topic	**Key Element**
Advanced VPN Concepts and Practices	IPsec Internet Key Exchange (IKE) IKE Key Exchange Process – Phase 1/ Phase 2 Stages
Remote Access VPNs	Connection Initiation Link Selection
Multiple Entry Point VPNs	How Does MEP Work Explicit MEP Implicit MEP
Tunnel Management	Permanent Tunnels Tunnel Testing VPN Tunnel Sharing Tunnel-Management Configuration Permanent-Tunnel Configuration Tracking Options Advanced Permanent-Tunnel configuration VPN Tunnel Sharing Configuration
Troubleshooting	VPN Encryption Issues
VPN Debug	vpn debug Command vpn debug on | off vpn debug ikeon |ikeoff vpn Log Files vpn debug trunc VPN Environment Variables vpn Command vpn tu Comparing SAs
Lab 5: Configure Site-to-Site VPNs with Third Party Certificates	Configuring Access to the Active Directory Server Creating the Certificate Importing the Certificate Chain and Generating Encryption Keys Installing the Certificate

	Establishing Environment Specific Configuration Testing the VPN Using 3rd Party Certificates
Lab 6: Remote Access with Endpoint Security VPN	Defining LDAP Users and Groups Configuring LDAP User Access Defining Encryption Rules Defining Remote Access Rules Configuring the Client Side

Table 5-1: Advanced IPsec VPN and Remote Access Topics

Sample CCSE Exam Question

Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?:

1. vpnd
2. cvpnd
3. fwm
4. fwd

Answer

Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?:

1. **vpnd**
2. cvpnd
3. fwm
4. fwd

Chapter 6: Auditing and Reporting

The SmartEvent Software Blade turns security information into action with realtime security event correlation and management for Check Point security gateways and third-party devices. SmartEvent's unified event analysis identifies critical security events from the clutter, while correlating events across all security systems. Its automated aggregation and correlation of data not only minimizes the time spent analyzing log data, but also isolates and prioritizes the real security threats. The SmartReporter Software Blade centralizes reporting on network, security, and user activity and consolidates the data into concise predefined and custom-built reports. Easy report generation and automatic distribution save time and money.

Objectives:

- Create Events or use existing event definitions to generate reports on specific network traffic using SmartReporter and SmartEvent in order to provide industry compliance information to management.
- Using your knowledge of SmartEvent architecture and module communication, troubleshoot report generation given command-line tools and debug-file information.

Topics

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

Topic	**Key Element**
Auditing and Reporting Process	Auditing and Reporting Standards
SmartEvent	SmartEvent Intro
SmartEvent Architecture	Component Communication Process Event Policy User Interface
SmartReporter	Report Types
Lab 7: SmartEvent and SmartReporter	Configure the Network Object in SmartDashboard Configuring Security Gateways to work with SmartEvent Monitoring Events with SmartEvent Generate Reports Based on Activities

Table 6-6: Using SmartUpdate Topics

Sample CCSE Exam Question

How many Events can be shown at one time in the Event preview pane?

1. 5,000
2. 30,000
3. 15,000
4. 1,000

Answer

How many Events can be shown at one time in the Event preview pane?

1. 5,000
2. **30,000**
3. 15,000
4. 1,000