



# Check Point Security Administrator R70

## Check Point Security Administration R70



<b>Length</b>	5 days* (recommended)
<b>Prerequisites</b>	Basic networking knowledge, knowledge of Windows Server and/or UNIX, and experience with TCP/IP and the Internet
<b>Take this class if</b>	<ul style="list-style-type: none"> <li>  You are a systems administrator, security manager, or network engineer who manages R70 Security Gateway deployments on open servers, IP appliances, UTM-1 appliances, or Power-1 appliances.</li> <li>  Want to earn Check Point Certified Security Administrator (CCSA) R70 certification</li> </ul>
<p>Check Point Security Administration R70 is a foundation course for Check Point's Security Management Systems, Security Gateway Systems, and deployment platforms. This course provides an understanding of basic concepts and skills necessary to configure Check Point Software Blades including Firewall, IPSEC VPN, IPS, Network Policy Management, Logging &amp; Status, and Monitoring, URL Filtering, Antivirus &amp; Anti-malware, Anti-spam &amp; Email Security. During this course, students will configure a Security Policy, secure communications across the Internet, defend against network threats, and learn about managing and monitoring a secure network.</p>	<ul style="list-style-type: none"> <li>  <b>More details</b></li> <li>  <a href="#">Table of Contents</a></li> <li>  <a href="#">Sample Chapter</a></li> <li>  <a href="#">Courseware Objectives</a></li> </ul>
<b>You will learn</b>	<ul style="list-style-type: none"> <li>  Design and install version R70 in a distributed environment</li> <li>  Perform a backup and restore the current installation.</li> <li>  Identify critical files</li> <li>  Deploy Gateways</li> <li>  Create and configure network, host and gateway objects.</li> <li>  Verify SIC establishment</li> <li>  Create a basic Rule Base</li> <li>  Configure NAT rules</li> <li>  Evaluate existing policies and optimize rules</li> <li>  Ensure seamless upgrades and minimal downtime.</li> <li>  Use queries to monitor IPS and common network traffic and troubleshoot events.</li> <li>  Generate reports, troubleshoot system and security issues, and ensure network functionality.</li> <li>  Configure alerts and traffic counters, monitor suspicious activity, analyze tunnel activity and monitor remote user access</li> <li>  Apply upgrade packages</li> <li>  Attach product licenses</li> </ul>

	<ul style="list-style-type: none"> <li>  Perform a pre-installation compatibility assessment</li> <li>  Centrally manage users and manage users' access using external databases.</li> <li>  Configure a pre-shared secret site-to-site VPN.</li> <li>  Configure a certificate based site-to-site VPN using an internal CA or a third party CA.</li> <li>  Configure permanent tunnels for remote access.</li> <li>  Configure VPN tunnel sharing.</li> <li>  Configure Check Point Messaging Security to test IP Reputation, content based anti-spam, and zero hour virus detection.</li> <li>  Configure a Web-filtering and antivirus policy to filter and scan traffic.</li> <li>  Implement default or customized profiles to designated Gateways.</li> <li>  Create and install IPS policies.</li> </ul>
<p><b>Exercises</b></p>	<ul style="list-style-type: none"> <li>  <b>Distributed Installation</b> <ul style="list-style-type: none"> <li>  Install and configure the Security Management Server</li> <li>  Install SecurePlatform on the Security Gateway</li> <li>  Configure the Security Gateway using WebUI</li> <li>  Launch SmartDashboard</li> </ul> </li> <li>  <b>Branch Office Security Gateway Installation</b> <ul style="list-style-type: none"> <li>  Configure Branch Gateway via WebUI</li> </ul> </li> <li>  <b>Command Line Interface (CLI) Tools</b> <ul style="list-style-type: none"> <li>  Initialize the ICA</li> <li>  Set expert password</li> <li>  Add and delete administrators</li> <li>  Run backup and restore</li> </ul> </li> <li>  <b>Defining Basic Objects</b> <ul style="list-style-type: none"> <li>  Create Security Gateway Object</li> <li>  Create Rules for Corporate Gateway</li> <li>  Create the Remote Security Gateway Object</li> </ul> </li> <li>  <b>Configure DMZ</b> <ul style="list-style-type: none"> <li>  Configure DMZ Interface on the Gateway</li> <li>  Create a DMZ Object</li> </ul> </li> <li>  <b>Configure NAT</b> <ul style="list-style-type: none"> <li>  Configure Hide NAT</li> <li>  Configure Static NAT</li> <li>  Observe NAT using fw monitor</li> </ul> </li> <li>  <b>Monitoring with SmartView Tracker</b> <ul style="list-style-type: none"> <li>  Launch SmartView Tracker</li> <li>  Track by Source and Destination</li> </ul> </li> <li>  <b>Using SmartUpdate</b> <ul style="list-style-type: none"> <li>  Get Gateway data and run Cpinfo</li> <li>  Download HFA Package</li> </ul> </li> <li>  <b>Upgrade a Security Gateway Locally</b></li> <li>  <b>Client Authentication</b> <ul style="list-style-type: none"> <li>  Configure Manual Client Authentication with FTP and Local User</li> <li>  Configure Partially Automatic Client Authentication</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>with LDAP</li><li>i Test Active Directory Authentication</li><li>i Create a Database Revision</li><li>i <b>Configure a Site-to-Site VPN</b><ul style="list-style-type: none"><li>i Define the VPN Domain</li><li>i Create the VPN Community</li><li>i Create VPN Rule</li><li>i Test VPN Connection</li><li>i VPN Troubleshooting</li></ul></li><li>i <b>Configure Two Gateway IKE Encryption Using Certificates</b><ul style="list-style-type: none"><li>i Save a Certificate for Export</li><li>i Add Machine to VPN Community</li><li>i Create a Certificate Authority</li><li>i Modify Rule Base</li><li>i Install and Verify Security Gateway Configuration</li><li>i Test Encryption with Certificates</li><li>i Revert to Standard Security Policy</li></ul></li><li>i <b>Remote Access and Office Mode</b><ul style="list-style-type: none"><li>i Create Remote Access Group</li><li>i Configure Gateway for IKE Encryption and LDAP Authentication</li><li>i Configure VPN Domain</li><li>i Configure Office Mode IP Pool</li><li>i Configure Remote Access Object</li><li>i Modify Rule Base for Remote Access</li><li>i Create a Site Using Site Wizard</li><li>i Verifying Office Mode IP Assignment</li><li>i Test Remote Connection</li></ul></li><li>i <b>Messaging and Content Security</b><ul style="list-style-type: none"><li>i Configure IPS for Preliminary Detection</li><li>i Analyze Attacks</li><li>i Reconfiguring IPS to Block Attacks</li><li>i Review Logs</li></ul></li></ul>
--	---

## Check Point Certified Security Administrator R70 (CCSA R70)

With over 24,000 CCSA certified professionals worldwide, CCSA certification is one of the most highly recognized and respected vendor-specific security certifications available.

The foundation of Check Point certifications, CCSA R70 certification validates a Security Administrator's ability to maintain day-to-day operation of Check Point security solutions and ensure secure access to information across the network. Proficiencies include creating and installing Security Policies, using logging and reporting features, and managing anti-spoofing, Network Address Translation (NAT), and OPSEC applications.

More information on specific topics, skills, and competencies covered by CCSA R70 certification is available in the course and exam details.

**Exam:**

#156-215.70

**Course:**

Check Point Security Administration R70

**Products:**

VPN-1, SmartCenter, SmartConsole, IPS

**Competencies:**

Backup and restore, monitoring tools, object creation, Rule Base construction, VPNs, NAT, authentication (including LDAP), user management

**Exam:156-215.70****Course:**

Check Point Security Administration R70

**Prepares you for Certifications:**

CCSA R70, CCSE R70

Passing exam #156-215.70 earns you "Check Point Certified Security Administrator R70 (CCSA R70)" certification.

<b>Objectives</b>	
	<ul style="list-style-type: none"> <li> <b>i Check Point Technology Overview</b> <ul style="list-style-type: none"> <li>i Describe Check Point's unified approach to network management, and the key elements of this architecture</li> <li>i Design a distributed environment using the network detailed in the course topology</li> <li>i Install the Security Gateway version R70 in a distributed environment using the network detailed in the course topology</li> </ul> </li> <li> <b>i Check Point Software Blades</b> <ul style="list-style-type: none"> <li>i Given CheckPoint's latest integration of CoreXL technology, select the best security solution for your corporate environment</li> </ul> </li> <li> <b>i Deployment Platforms</b> <ul style="list-style-type: none"> <li>i Given network specifications, perform a backup and restore the current Gateway installation from the command line</li> <li>i Identify critical files needed to purge or backup, import and export users and groups and add or delete administrators from the command line</li> <li>i Deploy Gateways using sysconfig and cpconfig from the Gateway command line</li> <li>i Use the Command Line to assist support in troubleshooting common problems on the Security Gateway</li> </ul> </li> <li> <b>i Introduction to the Security Policy</b> <ul style="list-style-type: none"> <li>i Given the network topology, create and configure network, host and gateway objects</li> <li>i Verify SIC establishment between the SmartCenter Server and the Gateway using SmartDashboard</li> <li>i Create a basic Rule Base in SmartDashboard that</li> </ul> </li> </ul>

- includes permissions for administrative users, external services, and LAN outbound use
- i Configure NAT rules on Web and Gateway servers
- i Evaluate existing policies and optimize the rules based on current corporate requirements
- i Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime
- i **Monitoring Traffic and Connections**
  - i Use queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data
  - i Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, and ensure network functionality
  - i 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
- i **Using SmartUpdate**
  - i Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications
  - i Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways
  - i Upgrade and attach product licenses using SmartUpdate
- i **Upgrading to R70**
  - i Based on current products or platforms used in an enterprise network, perform a preinstallation compatibility assessment before upgrading to R70
  - i Given R70 licensing restrictions, obtain a license key
  - i Install a Contract File on platforms such as Windows, SecurePlatform, Linux, Solaris and IPSO
- i **User Management and Authentication**
  - i Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely
  - i Manage users to access to the corporate LAN by using external databases
- i **Encryption and VPNs**
  - i Select the most appropriate encryption algorithm when securing communication over a VPN, based on corporate requirements
  - i Establish VPN connections to partner sites in order to establish access to a central database by configuring Advanced IKE properties
- i **Introduction to VPNs**
  - i Configure a pre-shared secret site-to-site VPN with partner sites
  - i Configure a certificate based site-to-site VPN using one

	<ul style="list-style-type: none"><li>partner's internal</li><li>i Configure a certificate based site-to-site VPN using a third-party CA</li><li>i Configure permanent tunnels for remote access to corporate resources</li><li>i Configure VPN tunnel sharing, given the difference between hostbased, subnet-based and gateway-based tunnels</li><li>i <b>Messaging and Content Security</b><ul style="list-style-type: none"><li>i Configure Check Point Messaging Security to test IP Reputation, content based anti-spam, and zero hour virus detection</li><li>i Based on network analysis disclosing threats by specific sites, configure a Web-filtering and antivirus policy to filter and scan traffic</li></ul></li><li>i <b>Check Point IPS</b><ul style="list-style-type: none"><li>i Implement default or customized profiles to designated Gateways in the corporate network</li><li>i Manage profiles by tracking changes to the network, including performance degradation, and troubleshoot issues with the network related to specific IPS policy rules</li><li>i Create and install IPS policies</li></ul></li></ul>
--	--

Take advantage of the latest special offers on R70 classes, and then register for training with an ATC near you!

\*Course length and price may vary by ATC. Please contact your local ATC for detailed information.

©2010 Check Point Software Technologies Ltd. All rights reserved.