

Check Point Certified Security Administrator (CCSA) R81

This entry-level CSSA training prepares security admins to install, configure and manage Check Point R81 security solutions including gateways, security policies, VPNs, threat prevention and advanced network protection features.

[CBT Nuggets course material](#) →

WEEK 1

Network and Security Refresher

164 min.

Topology and Traffic Flow	4
Network Address Translation (NAT)	8
Stateful vs Packet Filtering Firewalls	10
Virtual LANs (VLANs)	7
Virtual Private Network (VPN)	5
Intrusion Prevention System (IPS)	5
Validation	4

Getting To Know Check Point

CCSA Exam Objectives and CheckMates	5
Check Point Security Product Lineup	8
Security Gateway Software Blades	11
Check Point Deployment Methods	13
Physical Check Point Security Gateway Features	2
Check Point Licensing	12
Validation	4

Check Point Lab Setup

Introduction	1
Lab Topology and EVE-NG Overview	7
Installing the Gaia OS	11
Deploying A Windows OS In EVE-NG	11
Deploying a TinyCore Linux Web Server	7
Register For A Check Point Evaluation License	2
Validation	4

Deploying SMS and SGs

Introduction	1
Deploying Our Security Gateways	22

WEEK 2

151 min.

Touring the Security Gateway Interface	7
Configuring A Default Route On Our SGs	6
Deploying A Security Management Server (SMS)	6
Validation	4

Configuring Our SMS and SGs

Introduction	1
Installing the SmartConsole	7
Touring the SmartConsole	16
Adding HQ-SG-1 To Our HQ-SMS	4
Configuring Hide NAT and Security Policies	7
Adding Site_A-SG To Our HQ-SMS	13
Troubleshooting HQ-SMS To Site_A-SG Communications	19
Validation	4

Licensing and Policies

Introduction	1
Requesting Evaluation Licenses	5
Centralized Licensing Using SmartUpdate	6
Using Local Licensing	8
Access Control Policies	6
Threat Prevention Policies	8
Autonomous Policies	7
Validation	3

Intro To Access Control Policies

Introduction	1
Access Control Policies	9
Enabling ICMP On Security Gateways	3

WEEK 3

151 min.

Configuring Zone-Based ACPs	6
Configuring Time-Based ACPs	6
Inspection Profiles	6
Configuring Outbound HTTPS Inspection	14
Configuring Inbound HTTPS Inspection	7
Validation	4

Managing Access Control Policies

Introduction	1
Using ACP Sections	4
Using Policy Packages	15
Policy Layers	5
Inline Layers	8
Lab Update	25
Validation	4

Advanced Access Control Policies

Application Control Policies	15
URL Filtering Policies	9
Content Awareness Policies	8
Configuring Identity Awareness	14

WEEK 4**156 min.**

Identity Awareness Policies 10

Validation 4

Threat Prevention Policies and IPS

Introduction 1

Threat Prevention Blades 2

Threat Prevention Policy Rules 15

Intrusion Prevention System (IPS) Policies 11

Indicators of Compromise (IOC) 8

IPS Protections 9

Updating Your IPS 8

Testing Your IPS 8

Validation 6

Advanced Threat Prevention

Introduction 1

Configuring Anti-Bot & Anti-Virus 8

Testing Anti-Bot & Anti-Virus 8

Configuring Threat Emulation & Threat Extraction 17

Zero Phishing Blade 7

Configuring Zero Phishing 9

Validation 5

Access Control & Threat Prevention Adv. Settings

Introduction 1

Advanced Inspection Settings 9

App Control & URL Filtering Advanced Settings 9

WEEK 5**156 min.**

Content Awareness Advanced Settings 2

Threat Prevention Advanced Settings 6

Stealth Rules 6

Anti-Spoofing 9

Validation 7

Autonomous Policies and Email Security

Introduction 1

What Are Autonomous Policies? 4

Enabling Autonomous Threat Prevention 13

Managing Autonomous Threat Prevention From the CLI 4

Mail Filtering and MTA Gateways 8

Anti-SPAM & Email Security 8

Validation 4

Managing IPSec VPNs

Introduction 1

IPSec Virtual Private Networks (VPNs) 5

How VPNs Work 8

IPSec VPN Terms 5

Configuring An IPSec Site-To-Site VPN 20

Managing IPSec VPNs From the CLI 4

Validation 4

Mobile Access VPNs

Introduction 1

Types Of Mobile/Remote Access VPNs 5

Preparing Our Lab Environment For Mobile Access VPNs 3

Installing the Mobile Access Blade	4
VPN Community & Settings	8
Testing Our SSL VPN Portal	2
Access Control Policies For Remote Access	8
Installing and Testing Our Mobile Access VPN	6

WEEK 6

158 min.

Validation	5
------------	---

Additional Network Security Features

Introduction	1
GeoProtection	10
Quality of Service (QoS)	12
Monitoring Logs	6
SmartView Monitor	10
Data Loss Prevention (DLP)	22
Validation	4

NAT, VLANs, Bridging & Bonding

Introduction	1
Static NAT / Automatic NAT	8
No NAT	4
Manual NAT	5
Virtual LANs (VLANs)	8
Configuring VLANs	13
Bridging (AKA: Transparent Mode or Layer 2 Mode)	3
Bonding Interfaces	9
Validation	4

Managing User Accounts and Backups

Introduction	1
Managing Users & Roles On Appliances	7
Managing Users & Profiles Within SmartConsole	5
Managing Users From the Command Line	3
Snapshots, Backups and Saved Configurations	7
Creating Snapshots, Backups and Saved Configurations	10

WEEK 7

152 min.

Managing Snapshots, Backups and Saved Configurations From the CLI	10
Backing Up An SMS	4
Validation	4

Banners, Updates, Performance Tuning and IoT

Banner Messages and MOTD	4
Managing Device Updates	5
Upgrading Gaia OS	15
Performance Tuning Solutions	7
Check Point IoT Protect	8
Validation	4

ClusterXL and HA Gateway Deployment

Now that we've got our secondary gateway up and running it's time to build a cluster using ClusterXL. We're going to start by setting up an HA cluster using HQ-SG-1 and HQ-SG-2.	1
Cluster XL	7
Types Of Clusters	14
Reviewing the Cluster Topology	3

Setup Secondary Gateway	14
Configuring ClusterXL	21
Managing the Cluster	10
Testing Failover	2
Upgrading A Clusters' Gaia Version	2
Validation	5

Troubleshooting Check Point

Introduction	1
Important Processes and Daemons	8
The Policy Installation Work Flow	3

WEEK 8

34 min.

Useful CLI Commands	11
Errors About Blades	4
Checking the Status of SMS	3
Troubleshoot Lost Communications Between SMS and SGs	8
Help! I've Locked Myself Out Of My Gateway	4
Validation	4