



CHECK POINT

Check Point Security Expert R81.20 (CCSE) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

EXPERT

At a glance

COURSE	Check Point Security Expert R81.20 (CCSE)
TRACK	Check Point
DOMAIN	Cyber Security
LEVEL	Expert
DURATION	On request
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a expert course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

R81.20 is no longer Check Point's current training release. R82 is. Check Point retired the R81.20 certification exams on 30 June 2026 and replaced them with 156-315.82 for CCSE and 156-215.82 for CCSA. This map covers R81.20 because that is what this course targets, and because the R81.20 estates it describes are still in production across most of the customer base. If you need the current certification rather than the skills on the estate you run, you will be sitting the R82 exam — say so when you enrol and we will place you on the R82 map instead.

The twelve modules below take Check Point's own published course topics for Certified Security Expert R81.20, in the order Check Point publishes them. The lab exercises behind them are Check Point's own as well, and the course runs them in sequence rather than demonstrating them.

CCSE is where Check Point stops being a graphical interface and becomes a system. Most of the advanced material — acceleration, clustering, upgrade paths, the management API — is only learnable at the command line, and most of it is only learnable by breaking something first. The course is built accordingly: fewer slides than CCSA, considerably more expert mode.

Module 01 — Advanced Deployments

Upgrading and migrating a live management estate without losing the database or the weekend.

- Upgrade paths between R81.x versions, and reading Check Point's supported-path matrix before you plan anything
- CPUSE: importing a package, verifying it, and the difference between verify and install
- In-place upgrade against advanced upgrade with migration, and choosing between them honestly
- Migrate export and import to move a management database onto new hardware or a new version
- Pre-upgrade verification output, and treating its warnings as work rather than noise
- Rolling back: snapshot before the upgrade, and what reverting actually costs in downtime
- Post-upgrade validation — SIC, licences, policy install — before you declare it done
- Sequencing management and gateway upgrades, and the version-compatibility window in between

Module 02 — Management High Availability

A second management server, and what it does and does not protect you from.

- Primary and secondary Security Management Server roles, and what each holds
- Deploying a secondary server and establishing trust with the primary
- Database synchronisation: automatic and manual, and confirming it has actually happened
- Active and standby status, and the fact that the standby is read-only until promoted
- Promoting the secondary, and the steps to make gateways accept it
- Recovering the original primary and returning to the intended roles
- What management high availability does not give you: gateways keep enforcing without either server
- A dedicated log server alongside the pair, and separating logging load from management
- Testing failover deliberately, on a schedule, rather than discovering it during an incident

Module 03 — Advanced Gateway Deployment

Gateway-side upgrades and deployment at scale.

- Upgrading a Security Gateway from SmartConsole rather than one console session at a time
- The package repository on the management server, and pushing packages down to gateways
- Central Deployment for hotfixes and versions across multiple gateways
- Upgrading a cluster with connectivity maintained: the member order and the version pairing in between
- Zero-downtime and minimal-downtime cluster upgrade approaches, and the trade-off each makes
- Verifying gateway version, hotfix level and policy state after the upgrade
- Rolling back a gateway that came up wrong
- Planning a phased upgrade across an estate rather than a single flag day

Module 04 — Advanced Policy Configuration

Policy installation understood as a process, not a button.

- Policy types in a package, and what each installs onto the gateway
- The installation flow: verification, compilation, transfer, activation
- Accelerated policy installation, and what it changes about the transfer step
- Monitoring installation status per gateway and diagnosing the one target that fails
- Policy verification errors, and reading the compiler output instead of retrying
- Ordered and Inline Layers at expert level, including shared layers across packages
- Dynamic and updateable objects in policy, and how the gateway resolves them at runtime
- Management Data Plane Separation, and when a deployment needs it
- Policy installation on a cluster, and member behaviour during the install window

Module 05 — Advanced User Access Management

Identity as a policy criterion, sourced reliably.

- Identity Awareness architecture and the identity sources available
- The Identity Collector and the AD Query method, and choosing between them for a given site
- Browser-based authentication and captive portal, and where it is the only option that works
- Identity agents, and the environments that justify deploying software to endpoints
- Identity sharing between gateways, so a user identified once does not authenticate repeatedly
- Access roles in policy, and writing rules against people and machines rather than addresses
- Terminal server and shared-workstation identity, and its limits
- Diagnosing the user who is authenticated but not matching the rule you wrote

Module 06 — Custom Threat Protection

Tuning Threat Prevention until it is both effective and survivable.

- Threat Prevention profiles, and building your own rather than living on the defaults
- IPS protections: activation, performance impact, and the confidence and severity settings that govern them
- Anti-Bot and Anti-Virus, and what each one is actually looking at
- Threat Emulation and Threat Extraction, and the user-experience decision between them
- Exceptions and exception groups, scoped narrowly so they do not quietly disable the profile
- Protection updates and staged activation, so a new signature set does not take out a business application

- Detect against Prevent, and a rollout that earns its way to Prevent
- Reading a Threat Prevention log and deciding whether it is a detection or a false positive
- Measuring the performance cost of each blade on a live gateway

Module 07 — Advanced Site-to-Site VPN

Site-to-site tunnels beyond the simple two-gateway case.

- IKEv1 and IKEv2, phase 1 and phase 2, and the parameters that must match on both ends
- VPN communities: meshed and star, and the topology each one suits
- Domain-based against route-based VPN, and the VPN Tunnel Interface
- Interoperable devices: building a tunnel to a non-Check Point peer, and the encryption domain mismatch that will stop it
- Permanent tunnels, tunnel monitoring and dead peer detection
- Link Selection, and VPN across multiple external interfaces
- NAT and VPN together, and the traffic that should not be translated
- Troubleshooting with vpn tu, IKE debugs, and reading phase 1 failures against phase 2 failures
- Certificate-based against pre-shared key authentication, and the case for certificates

Module 08 — Remote Access VPN

Bringing users in, with the client decisions that come with it.

- Remote Access VPN architecture and the Remote Access community
- Client options and the licensing each one requires
- Authentication methods: directory, certificate, multifactor, and combining them
- Office mode address assignment, and the routing that must exist for it to work
- Split tunnelling against full tunnelling, and defending whichever one you chose
- Access control for remote users, and using access roles rather than the office mode pool
- A remote access gateway cluster, and what the client experiences during a failover
- Diagnosing the client that connects but cannot reach anything

Module 09 — Mobile Access VPN

Clientless and portal-based access, which follows different rules.

- Mobile Access blade architecture, and how it differs from Remote Access VPN
- The Mobile Access portal, and publishing applications through it
- Web applications, file shares and native applications as portal resources
- Authentication and authorisation for portal users
- The Mobile Access policy, and its relationship to the access control policy
- Endpoint compliance checks before access is granted
- Certificate and portal customisation, and the trust the browser needs
- Diagnosing a published application that loads for one user and not another

Module 10 — Advanced Security Monitoring

Turning log volume into something a person can act on.

- Dedicated log server deployment, and moving logging load off the management server

- Log indexing and the search behaviour that depends on it
- SmartEvent deployment: correlation unit, server and the roles they play
- Event definitions, and tuning correlation so the event list stays readable
- SmartEvent views, reports and statistics, and scheduling the ones that get read
- Compliance monitoring, and checking the estate against a baseline rather than by eye
- Forwarding to an external SIEM, and deciding what belongs there against what stays in SmartEvent
- Log retention, disk sizing and what happens when the log partition fills

Module 11 — Performance Tuning

Where the throughput went, and how to get it back.

- The packet flow through the gateway, and the stages that can and cannot be accelerated
- SecureXL: templates, accept templates, drop templates, and the rules that break templating
- CoreXL, firewall instances and the split between SND and instance cores
- Multi-queue on the interfaces, and when the interrupt handling is the bottleneck
- Dynamic Dispatcher and connection distribution across instances
- Measuring before you tune: cpview, fw ctl multik stat, and interface counters
- Finding the elephant flow, and the rule or blade that is doing the damage
- HTTPS Inspection and Threat Prevention as the usual causes, and the bypass decisions available
- Verifying the improvement with the same measurement you started from

Module 12 — Advanced Security Maintenance

The command-line and automation layer that separates an expert from an administrator.

- Gaia clish and expert mode, and the tasks that genuinely require each
- Check Point processes, cpwd_admin, and what a watchdog restart is telling you
- fw ctl, fw monitor and cpview as a diagnostic set rather than individual commands
- The Gaia API and the Management API: authentication, sessions and publishing changes
- Scripting bulk changes through the API instead of clicking them, and testing on a clone first
- SmartTasks, and triggering a script on a management event
- Bash scripting on the appliance, and keeping scripts somewhere an upgrade will not remove them
- Health checks you can schedule, so problems arrive as a report rather than an outage

Who should take this

Engineers who already hold CCSA, or who administer a Check Point estate daily and could pass CCSA tomorrow. Check Point states CCSA training or certification as the prerequisite, and it is a real one: this course opens assuming you can build a policy, configure NAT and establish SIC without being walked through it.

Beyond that, Check Point expects fundamental Unix and Windows knowledge, certificate management experience, and system administration and TCP/IP networking background. The Unix expectation is the one people underestimate. A large part of CCSE happens in expert mode, and if the Linux shell is unfamiliar you will spend the week learning bash instead of learning Check Point.

It suits engineers who own upgrades, clusters and VPN interconnects, and consultants who have to walk into an unfamiliar estate and diagnose it quickly.

The exam

The CCSE R81.20 exam is set and awarded by Check Point and delivered at Pearson VUE test centres.

- Exam code 156-315.81.20
- Delivered through Pearson VUE
- CCSA is the stated prerequisite
- Retired by Check Point on 30 June 2026, replaced by 156-315.82 for CCSE R82
- Check Point also publishes a paid practice exam, 156-610, for the R82 version

Check Point publishes question count, time limit and passing score in its own CCSE exam prep guide. We do not restate those figures here, because we will not print numbers we cannot source directly from Check Point's current published guide — download it from Check Point before you book, and confirm the figures for the version you are sitting.

The exam is purchased separately from Check Point. We arrange the voucher on your behalf and send you the details, and you choose your own exam date.

How we deliver it

Three days, classroom or online live, or at your office for a private group. Each delegate gets a pod large enough to hold a management pair, a gateway cluster and a VPN peer, because clustering and management high availability cannot be taught on a single box.

The teaching weight sits at the command line. Expect to spend the second and third days mostly in expert mode: acceleration measurement, cluster failover, VPN debugs and the management API. Topic checkpoints each day, and a final-afternoon scenario where you are given an estate with three unrelated faults and a time limit.

Mapped to Check Point's published course topics for Certified Security Expert R81.20. Taught from Hacky Security's own curriculum and lab estate by instructors who upgrade and troubleshoot Check Point clusters for a living. These are our own preparation courses; they are not official Check Point courseware and we are not a Check Point Authorised Training Centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/checkpoint-check-point-security-expert-r81-20-ccse/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.