



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com

Phone: +46 8 555 188 00



Check Point VPN Specialist (CPVS) R82

CODE:	LENGTH:	PRICE:
CKT_CPVS_R82	24 Hours (3 days)	kr26,500.00

Description

This course provides intermediate knowledge and hands-on experience in designing, configuring, and troubleshooting secure VPN solutions. You explore Site-to-Site, Remote Access, and Mobile Access VPN deployments. The course covers key technologies such as IPSec and IKE/IKEv2, VPN Communities, authentication methods, and encryption domains, with advanced topics like NAT integration, PKI, high availability, and SD-WAN. Through practical labs and real-world scenarios, participants develop the skills required to implement, manage, and troubleshoot secure VPN environments.

Objectives

Module 1: Check Point VPN Solution Overview

- Identify the core components of the Check Point VPN solution.
- Explain the differences between Site-to-Site, Remote Access, and Mobile Access VPN deployments.
- Describe the encryption and key-exchange protocols used in Check Point VPNs.
- Explain how Access Control policies affect VPN traffic flow.

Lab tasks

- Examine the existing VPN Configuration
- Update the VPN to Use IKEv2
- Verify VPN Operation

Module 2: Site-to-Site VPN Configuration

- Explain Site-to-Site VPN basics, deployment, and communities.
- Describe pre-shared keys and certificates used to authenticate with third-party and externally managed VPN Gateways.
- Explain Link Selection.
- Explain tunnel management features.

Lab tasks

- Review the existing VPN Community
- Modify the Topology (Mesh to Star)
- Verify the VPN
- Configure Fundamental Routing Settings
- Edit the VPN Community
- Modify the Access Control Policy
- Verify the Route-Based VPN

Module 3: Advanced Site-to-Site VPN Configuration

- Describe when externally managed certificate authentication is required.
- Explain policy requirements for VPN routing (bidirectional rule coverage on the central Gateway).
- Analyze key design factors for VPN and NAT integration.
- Compare ISP Redundancy and SD-WAN use cases.
- Implement a trusted external Certificate Authority (CA) trust workflow.

Lab tasks

- Review Route-Based VPN configuration
- Reconfigure BGP Routing
- Configure Route Redistribution
- Verify VPN and Dynamic Routing
- Configure Route-Based VPN with a Third-Party Peer
- Configure BGP Communication
- Modify OSPF Route Redistribution
- VPN and Dynamic Routing

Module 4: Remote Access VPN Configuration

- Describe Check Point Remote Access solutions and how they differ from each other.
- Describe how client security can be provided by Remote Access VPN.
- Compare authentication methods and determine the appropriate option for a given deployment.

- Describe Remote Access connectivity features, including Office Mode, Visitor Mode, and Hub Mode.
- Explain Multiple Entry Point (MEP).
- Configure a Remote Access VPN using SmartConsole.

Lab tasks

- Configure Remote Access VPN
- Configure Office Mode
- Configure and Verify Local User Authentication
- Configure and Verify Active Directory Authentication
- Verify Access to Internal Resources

Module 5: Advanced Remote Access VPN

- Explain how Multiple Entry Points (MEP) improve Remote Access VPN availability.
- Describe how Visitor Mode affects gateway selection and failover in MEP environments.
- Explain how multiple login options work in Remote Access VPN authentication.
- Describe certificate parsing and its role in user identity mapping.
- Explain how advanced authentication methods (DynamicID and machine authentication) enhance security.

Lab tasks

- Review Remote Access VPN
- Prepare Site Bravo
- Enable Multiple Entry Point
- Update Bravo Policy
- Validate Primary Connectivity
- Validate Failover

Module 6: Mobile Access VPN

- Explain how the Mobile Access Software Blade (MAB) secures remote communications.
- Identify and differentiate Mobile Access features including portals, link translation, native applications, and reverse proxy.
- Describe the Mobile Access security policy models.
- Describe the additional Mobile Access protections, including endpoint compliance scanning and Secure Workspace.

Lab tasks

- Enable Mobile Access VPN
- Configure Mobile Access Authentication
- Configure Mobile Access Policy
- Deploy the Guacamole Web Application
- Configure Native Application Access to A-Host
- Verify Mobile Access VPN Connectivity

Module 7: VPN Troubleshooting

- Identify and use the appropriate troubleshooting and debug commands/tools to resolve VPN troubleshooting issues.
- Understand the layered VPN troubleshooting methodology to isolate issues across Phase 1 (IKE), Phase 2 (IPSec), and traffic flow.
- Describe the roles of the Check Point VPN Daemons — IKED and VPND — and the VPN kernel module in tunnel negotiation and traffic handling.
- Understand how the debug workflow captures logs for tunnel-establishment and traffic-processing issues.
- Differentiate between IKEv1 and IKEv2 negotiation phases when analyzing VPN troubleshooting information.
- Recognize common VPN failure conditions and the tools used to investigate them.

Lab tasks

- Set the Stage
- Troubleshoot Remote Access Traffic
- Troubleshoot Alpha to Bravo Traffic
- Troubleshoot Alpha to Charlie Traffic
- Verify Restored Functionality
- Restore the Environment

Audience

- Security Administrators; Security Engineers
- Security Consultants; Security Architects

Prerequisites

Solid knowledge

- Unix-like and/or Windows operating systems
- Internet
- Networking Fundamentals
- Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS
- Six months minimum practical experience with Check Point Security Management

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
07 Dec 2026	EMEA ONLINE (CET / UTC +1)	CET	English	Instructor Led Online		kr26,500.00

Ytterligare information

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)