Over 35 Years Of Technology Training

Document Generated: 01/18/2025

Learning Style: Virtual Classroom

Provider: Citrix

Difficulty: Intermediate

Course Duration: 3 Days

Next Course Date: February 3, 2025

Check Point Certified Security Administrator (R81.x)

About this Course:

The Check Point Certified Security Administrator (CCSA) R81.x course is designed to provide participants with the essential knowledge and skills needed to configure

and manage Check Point Security Gateway and Management Software Blades.

Course Objectives:

- Describe the primary components of a Check Point Three-TierArchitecture and explain how they work together in the CheckPoint environment.
- Explain how communication is secured and how traffic is routed inthe Check Point environment.
- Describe the basic functions of the Gaia operating system.•Identify the basic workflow to install Security Management Serverand Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization’stopology for use in policies and rules.
- Identify the tools available to manage Check Point licenses andcontracts, including their purpose and use.
- Identify features and capabilities that enhance the configurationand management of the Security Policy.
- Explain how policy layers affect traffic inspection.•Articulate how Network Address Translation affects traffic.
- Describe how to configure manual and automatic Network AddressTranslation (NAT).
- Demonstrate an understanding of Application Control & URL Filteringand Autonomous Threat Prevention capabilities and how to configurethese solutions to meet an organization’s security requirements.
- Articulate how pre-shared keys and certificates can be configured toauthenticate with third party and externally managed VPN Gateways.
- Describe how to analyze and interpret VPN tunnel traffic.
- Configure logging parameters.•Use predefined and custom queries to filter log results.
- Identify how to monitor the health of supported Check Point hardwareusing the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point systeminformation and discuss best practices and recommendations foreach method.

Audience:

Technical professionals who support, install deploy or administer Check Point products.

Prerequisites:

Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.

Course Outline:

1. Describe Check Point's unified approach to network management and its

key elements
2. Design a distributed environment
3. Install the Security Gateway in a distributed environment
4. Perform a backup and restore the current Gateway installation from the command line
5. Identify critical files needed to purge (or backup), import and export users and groups, and add (or delete) administrators from the command line
6. Deploy Gateways using the Gaia web interface
7. Create and configure network, host, and gateway objects
8. Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard
9. Create a basicRule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use
10. Configure NAT rules on Web and Gateway servers
11. Evaluate existing policies and optimize the rules based on corporate requirements
12. Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades with minimal downtime
13. Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data
14. Use packet data to generate reports, troubleshoot system and security issues, and ensure network functionality
15. 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
16. Monitor remote gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications
17. Use SmartUpdate to apply upgrade packages to single or multiple VPN-1Gateways
18. Upgrade and attach product licenses using SmartUpdate
19. Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely
20. Manage users to access the corporate LAN by using external databases
21. Use Identity Awareness to provide granula- level access to network resources
22. Acquire user information used by the Security Gateway to control access
23. Define access roles for use in an Identity Awareness rule
24. Implement Identity Awareness in the Firewall Rule Base
25. Configure a pre-shared secret site-to-site VPN with partner sites
26. Configure permanent tunnels for remote access to corporate resources
27. Configure VPN tunnel sharing, given the difference between host-based, subunit-based, and gateway- based tunnels

Hands On Labs

Lab 1: Distributed Installations
Lab 2: Stand-alone Security Gateway Installations
Lab 3: Common Tools
Lab 4: Building a Security Policy
Lab 5: Configure the DMZ

Lab 6: Configure NAT
Lab 7: Monitor with SmartView Tracker
Lab 8: Client Authentication
Lab 9: Identity Awareness
Lab 10: Site-to-Site VPN between corporate and branch office

Return to Top
