

Check Point Certified Security Administrator (CCSA)

Course outline

After successful completion of CCSA, student will be able to defend against network threats, security gateway in a distributed environment, Schedule backups and seamless upgrades, Protect email and messaging content, Monitor suspicious network activities and analyze attacks, Troubleshoot network connections.

Prerequisite

- CCNA

Syllabus

Describe Check Point's unified approach to network management.

- Design a distributed environment using the network detailed in the course topology.
- Install the Security Gateway version R77 in a distributed environment using the network detailed in the course topology.
- Given network specifications, perform a backup and restore the current Gateway installation from the command line.
- Identify critical files needed to purge or backup, import and export users and groups and add or delete administrators from the command line.
- Deploy Gateways using sysconfig and cpconfig from the Gateway command line.
- Given the network topology, create and configure network, host and gateway objects. Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard.
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use.
- Evaluate existing policies and optimize the rules based on current corporate requirements.
- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime.
- Configure NAT rules on Web and Gateway servers.

- Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data.
- Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, and ensure network functionality.
- 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.
- Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications.
- Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways.
- Upgrade and attach product licenses using SmartUpdate.
- Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely.
- Manage users to access to the corporate LAN by using external databases.
- Use Identity Awareness to provide granular level access to network resources.
- Acquire user information used by the Security Gateway to control access.
- Define Access Roles for use in an Identity Awareness rule.
- Implementing Identity Awareness in the Firewall Rule Base.
- Configure a pre-shared secret site-to-site VPN with partner sites.
- Configure permanent tunnels for remote access to corporate resources.
- Configure VPN tunnel sharing, given the difference between host-based, subunit-based and gateway-based tunnels.
- Resolve security administration issues.