Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

Check Point Security Administration R77 (CCSA R77)

Course Main Topics:
Introduction to Check Point Technology
Deployment Platforms
Introduction to the Security Policy
Monitoring Traffic and Connections
Network Address Translation
Using SmartUpdate
User Management and Authentication
Identity Awareness
Introduction to Check Point VPNs
Certification
This course helps prepare for CCSA exam #156-215.77 available at VUE test centers www.vue.com/checkpoint. It contains 90 multiple-choice, scenario-based questions. A passing score is 70% or higher in 120 minutes.

Détails

- Code : PROD-CCSA
- Durée : 3 jours (21 heures)

Public

Pré-requis

Objectifs

Programme

Describe Check Point's unified approachto network management, and the key elements of it

- Design a distributed environment
- Install the Security Gateway in a distributed environment
- 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 the Gaia web interface
- 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
- Configure NAT rules on Web and Gateway servers
- 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 with minimal downtime
- Use Queries in SmartView Tracker to monitor IPS and common network traffic and trouble¬shoot events using packet data
- Use packet data to generate reports, trouble¬shoot system and security isues, 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
- 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 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
- Implement 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

LAB EXERCISES INCLUDE

- Distributed Installations
- Stand-alone Security Gateway
- Installations

- Common Tools
- Building a Security Policy
- Configure the DMZ
- Configure NAT
- Monitor with SmartView Tracker
- Client Authentication
- Identity Awareness
- Site-to-Site VPN between corporate and branch office

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages