

Check Point Security Administration NGX I

1. Show how VPN-1 NGX components and Check Point's Secure Virtual Network Architecture protect critical information assets.
2. Create rules and modify a Security Policy's properties.
3. Use advanced NGX features to minimize the information-security management burden, when working with objects and rules.
4. Use monitoring tools to track, monitor, and account for all connections logged by Check Point components.
5. Protect organizations from known network attacks and entire categories of emerging or unknown attacks, using SmartDefense.
6. Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations.
7. Identify and address NGX security issues, including encryption and Virtual Private Networks.
8. Verify the identity of users logging in to NGX, using NGX authentication schemes.
9. Implement LDAP, and integrate it with NGX SmartCenter Server.
10. Back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers.