

Barracuda Certified Engineer (BCE) Training

COURSE CONTENT

GET IN TOUCH



Multisoft Systems
B - 125, Sector - 2, Noida



(+91) 9810-306-956



info@multisoftsystems.com



www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The Barracuda Certified Engineer (BCE) Training by Multisoft Systems is designed to help IT professionals, network administrators, and cybersecurity engineers gain in-depth knowledge of Barracuda security solutions and enterprise-grade network protection technologies. This comprehensive training program focuses on firewall configuration, VPN management, intrusion prevention, email security, web filtering, application control, and advanced threat protection using Barracuda platforms.

Module 1: Introduction to Barracuda Security Solutions

- ✓ Overview of Barracuda Networks
- ✓ Understanding enterprise cybersecurity concepts
- ✓ Barracuda product portfolio and use cases
- ✓ Network security fundamentals
- ✓ Security threats and attack vectors
- ✓ Introduction to firewall technologies

Module 2: Barracuda Firewall Fundamentals

- ✓ Barracuda Firewall architecture
- ✓ Deployment models and installation
- ✓ Initial firewall configuration
- ✓ Interface configuration and network setup
- ✓ Routing and NAT concepts
- ✓ Firewall management console overview

Module 3: Network Configuration and Administration

- ✓ IP addressing and subnetting
- ✓ VLAN configuration
- ✓ DNS and DHCP settings
- ✓ Static and dynamic routing
- ✓ High availability and failover configuration
- ✓ Load balancing concepts

Module 4: Firewall Policies and Access Control

- ✓ Creating firewall rules and policies
- ✓ Access control management
- ✓ User authentication methods
- ✓ Identity and access management concepts

- ✓ Traffic filtering and packet inspection
- ✓ Policy optimization techniques

Module 5: VPN Configuration and Secure Remote Access

- ✓ VPN fundamentals
- ✓ Site-to-site VPN configuration
- ✓ Remote access VPN setup
- ✓ SSL VPN and IPSec VPN
- ✓ Secure remote connectivity management
- ✓ VPN troubleshooting techniques

Module 6: Intrusion Prevention and Threat Protection

- ✓ Intrusion Prevention System (IPS) concepts
- ✓ Malware and ransomware protection
- ✓ Threat intelligence integration
- ✓ Advanced threat protection configuration
- ✓ Content filtering and URL filtering
- ✓ Web security management

Module 7: Email Security and Protection

- ✓ Email security fundamentals
- ✓ Spam filtering configuration
- ✓ Anti-phishing protection
- ✓ Malware scanning for emails
- ✓ Email encryption concepts
- ✓ Managing email security policies

Module 8: Web Security and Application Control

- ✓ Web filtering policies

- ✓ Application visibility and control
- ✓ Bandwidth management
- ✓ Application-based traffic rules
- ✓ Safe browsing implementation
- ✓ HTTPS inspection and SSL management

Module 9: Monitoring, Logging, and Reporting

- ✓ Security event monitoring
- ✓ Log management and analysis
- ✓ Dashboard configuration
- ✓ Alert and notification settings
- ✓ Reporting and compliance management
- ✓ Traffic and threat analytics

Module 10: Firewall Troubleshooting and Maintenance

- ✓ Diagnosing network and firewall issues
- ✓ Packet capture and traffic analysis
- ✓ Troubleshooting VPN connectivity
- ✓ System backup and restore
- ✓ Firmware upgrades and patch management
- ✓ Performance optimization techniques

Module 11: Security Best Practices and Compliance

- ✓ Enterprise security best practices
- ✓ Security hardening techniques
- ✓ Compliance and governance concepts
- ✓ Risk management fundamentals
- ✓ Backup and disaster recovery planning
- ✓ Security audit preparation

Module 12: Hands-on Labs and Real-Time Projects

- ✓ Real-world firewall deployment scenarios
- ✓ Security policy implementation exercises
- ✓ VPN configuration labs
- ✓ Threat monitoring practical sessions
- ✓ Firewall troubleshooting case studies
- ✓ End-to-end enterprise security project