Course Duration: 20 hours (3 days)

Barracuda Control Panel and Email Security Administration

This course offers comprehensive training on Barracuda's Email-based security solutions, including email protection, impersonation defense, automated incident response, domain fraud protection, awareness training, compliance archiving, SaaS backup, data governance, and Zero Trust Access. Participants will gain a centralized understanding of Barracuda's integrated approach to modern cybersecurity, learn how to deploy and manage each module, and strengthen their organization's email and data infrastructure against evolving threats.

Course objectives

By the end of this course, participants will be able to:

- Configure and administer Barracuda Email Gateway Defense for inbound and outbound email security.
- Enable impersonation and account takeover protection across business email environments.
- Manage incident response workflows including threat detection, remediation, and reporting.
- Deploy DMARC authentication and prevent domain spoofing with Domain Fraud Protection.
- Launch security awareness campaigns and evaluate employee risk posture.
- Enable long-term email archiving and retention for regulatory compliance.
- Protect Microsoft 365 data using Cloud-to-Cloud Backup for Exchange, SharePoint, OneDrive, and Teams.
- Inspect and classify sensitive content in cloud storage to meet compliance requirements.
- Implement Zero Trust Access with device posture enforcement and identity-aware web filtering.

Prerequisites

- Basic understanding of email protocols (SMTP, POP/IMAP), DNS fundamentals (especially MX records), and general networking concepts.
- Prior experience with email server administration (e.g., Microsoft Exchange or Microsoft 365) or other email security solutions is recommended but not required.

- Familiarity with basic security terminology (malware, phishing, encryption) is beneficial for understanding the course material.

Target Audience

- IT Administrators
- Email Administrators
- Security Engineers
- Compliance Managers
- Technical Support Personnel

Course Outline

Module 1 Introduction to Barracuda Cloud Control and Security Services

- Overview of Barracuda Networks and Cloud Security Portfolio
- Accessing and Navigating the Cloud Control Portal

Module 2: Barracuda Email Gateway Defense (Formerly Email Security)

- Email Gateway Defense Features
- Administration and User Management
- Inbox Filtering
- Advanced Threat Protection
- Email Authentication
- Encryption and Data loss prevention
- End User Training

Module 3: Impersonation Protection (Formerly Sentinel) & Domain Fraud Protection

- Impersonation protection functionality
- Understanding Impersonation Protection operations
- Account take-over protection and reporting
- Product Connectivity and feature comparison
- Domain Fraud Protection Functions
- How Extension Protocols work.

Module 4: Incident Response

- Introducing Incident Response Functionality
- Insights and Reporting with Incident Response
- Automated Remediation
- Incident Review and remediation
- Automated Workflows
- Interconnectivity and feature comparison

Module 5: Security Awareness Training (Formerly Barracuda Phish Line)

- Security Awareness Training Overview
- Address Books
- Campaigns and Content Center
- Results Page overview
- Training features, Routine and LMS Integration

Module 6: Cloud Archiving Service

- Cloud Archiving Service Introduction
- Deployment and Integration
- Cloud Archiving Service End user access
- Creating Policies and Managing Retention

Module 7: Cloud to Cloud Backup

- Introduction to Barracuda Cloud to Cloud Backup
- Getting Started with Cloud-to-Cloud Backup

Module 8: Data Inspector

- Introducing data inspector features and functions
- Getting started with data Inspector

Module 9: Zero Trust Access (Formerly CloudGen Access)

- Zero Trust Access Features Overview
- Getting Started with zero Trust Access