

# **Symantec ProxySG 7.3 Administration with Secure Web Gateway**

Course Content –

Module 1: Introduction to the Symantec Secure Web Gateway

- Overview of the Symantec Secure Web Gateway family of products
- Introduction to the ProxySG, including key features, SGOS, the Global Intelligence Network, and management consoles

Module 2: Intercept traffic and apply policy

- Proxy services
- Writing policies in the Visual Policy Manager

Module 3: Apply security and web usage policy to encrypted traffic

- Key components of SSL encryption
- Managing SSL traffic with the ProxySG Integrating the SSL Visibility Appliance

Module 4: Provide security and web usage policies based on role or group

- Authentication on the ProxySG
- Authentication realms, credentials, and modes

Module 5: Enforce corporate guidelines for acceptable Internet browsing behaviour

- Determine appropriate use guidelines
- Write appropriate use policies

Module 6: Protect the endpoint from malicious activity

- Writing security policies using threat risk levels
- Ensuring safe downloads

Module 7: Centrally manage, monitor, and report on security activity

- Using Management Center to manage ProxySGs
- Using the SG Admin Console

Module 8: Maintaining the ProxySG, Management Center, and Reporter for optimal performance

- Monitoring the ProxySG within Management Center
- Using built-in health checks on devices

Module 9: Prevent malware and phishing threats while allowing broad web access

- Symantec Web Isolation fundamentals
- Isolation options for protecting privileged users and defending against phishing attacks
- Authentication in explicit and transparent proxy modes

Module 10: Enhance security by adding virus scanning and sandboxing with Content Analysis

- Virus scanning and sandboxing with Content Analysis
- Scanning best practices

Module 11: Expand security capabilities with cloud integrations

- Integrating Web Security Service
- Integrating CloudSOC Audit

Module 12: Course review

- Generating reports in Reporter