

SYMANTEC PROXY SG V6.6: BASIC ADMINISTRATION

DURATION: 2 DAYS

COURSE OVERVIEW

The Proxy SG 6.6 Basic Administration course is an introduction to deployment options and management of the individual key features offered using the Proxy SG 6.6 solution. This is an introductory course and is designed for students who are new to the Proxy SG solution.

TARGET AUDIENCE

The Proxy SG 6.6 Basic Administration course is intended for students who wish to master the fundamentals of the Proxy SG. It is designed for students who have not taken any previous training courses about the Proxy SG.

COURSE OBJECTIVES

1. Describe the major Secure Web Gateway functions of the Proxy SG
2. License and configure a Proxy SG
3. Deploy a Proxy SG in either explicit or transparent mode
4. Use the Visual Policy Manager to write policies to manage web filtering, authentication, and SSL traffic management
5. Use Proxy SG access logs to generate reports.

COURSE CONTENT

Module 1: Introduction to the Symantec Proxy SG Secure Web Gateway

1. Describe the functions of a proxy server
2. Differentiate proxy servers from firewalls
3. Describe the key features and benefits of the Proxy SG
4. List the various Proxy SG models
5. Access online Symantec community resources

Module 2: Proxy SG Security Deployment Options

1. Describe the three network deployment methods
2. Describe the three possible roles of the Proxy SG

Module 3: Proxy SG Management Console

1. Describe the relationship between the Management Console and the Proxy SG CLI
2. Describe the primary function of the major areas of the Management Console
3. Use the Management Console to access on-box help and Symantec product documentation

Module 4: Traffic Interception Using Proxy Services

1. Understand the functions of proxy services, listeners, and proxy types
2. Describe the three most common proxy services
3. Explain how the intercept and bypass settings affect what happens to network traffic passing through the Proxy SG
4. Explain the function of common global proxy service settings

Module 5: Hypertext Transfer Protocol

1. Understand how a connection is initiated over the transport layer
2. Identify the components of an HTTP URL
3. Explain the two types of HTTP messages: request and response
4. Identify common response codes

Module 6: Introduction to the Visual Policy Manager

1. Describe the relationship among the VPM, CPL, and the Management Console
2. Describe the default processing order for policy layers and rules
3. Describe triggers and actions that can be used in writing policy
4. Identify the types of objects that the VPM supports
5. Describe some of the best practices to be followed when using the VPM to create policy

Module 7: Filtering Web Content

1. Describe the main concepts of web filtering
2. Describe the primary category databases
3. Describe the category types available to policy
4. Describe how Web Filter and Web Pulse work together

Module 8: Using Threat Intelligence to Defend the Network

1. Understand Intelligence Services as provided by the Global Intelligence Network
2. Understand Geolocation and Threat Risk Levels and how they can be used in policy

Module 9: Ensuring Safe Downloads

1. Describe how malware can be transmitted via HTTP
2. Explain the methods, advantages, and disadvantages of file type detection
3. Describe some of the considerations in deciding what content to block as possible malware sources

Module 10: Notifying User of Internet Usage Policies

1. Explain the function and various components of built-in and custom exception pages
2. Describe the function of Notify User objects
3. Identify the types of pages that can be sent to users by using Notify User objects
4. Describe splash pages and coaching pages using Notify User objects in the VPM

Module 11: Access Logging on the Proxy SG

1. Describe, at a high level, how the Proxy SG performs access logging
2. Describe the components of a Proxy SG access log facility
3. Identify default log facilities and log formats
4. Describe common use cases for periodic and continuous uploading of access logs

Appendix A: Proxy SG Initial Configuration

Appendix B: IPv6 in Proxy SG Deployments

COURSE PREREQUISITES

This course assumes that students have a basic understanding of networking concepts, such as local-area networks (LANs), the Internet, security, and IP protocols.