

ProxySG 6.7 Advanced Administration

Course Summary

Description

The ProxySG 6.7 Advanced Administration course is intended for IT professionals who wish to learn to master the advanced features of the ProxySG.

Objectives

After taking this course, students will be able to:

- Solve common authentication and SSL issues
- Understand the underlying architecture of SGOS
- Monitor and analyze ProxySG performance
- Use policy tracing as a troubleshooting tool

Topics

- Using Authentication Realms
- Understanding Authentication Credentials
- Understanding Authentication Modes
- Understanding HTTPS
- Managing SSL Traffic on the ProxySG
- Optimizing SSL Interception Performance
- SGOS Architecture
- Caching Architecture
- System Diagnostics
- Introduction to Content Policy Language (CPL)
- Using Policy Tracing for Troubleshooting
- ProxySG Integration

Audience

This course is for IT network or security professionals who have practical experience with the ProxySG in the field and wish to master the advanced network security of the ProxySG.

Prerequisites

Before taking this course, you must have working knowledge of ProxySG Administration and should possess advanced knowledge of networking, security, and authentication.

Duration

Two days

ProxySG 6.7 Advanced Administration

Course Outline

- I. Using Authentication Realms**
 - A. Describe the benefits of enabling authentication on the ProxySG
 - B. Describe, at a high level, the ProxySG authentication architecture
 - C. Understand the use of IWA realms, with both IWA Direct and IWA BCAA connection methods
- II. Understanding Authentication Credentials**
 - A. Describe how NTLM and Kerberos authentication work in both IWA direct and IWA BCAA deployments
 - B. Configure the ProxySG to use Kerberos authentication
- III. Understanding Authentication Modes**
 - A. Describe authentication surrogates and authentication modes
 - B. Describe ProxySG authentication in both explicit and transparent deployment mode
- IV. Understanding HTTPS**
 - A. Describe key components of SSL encryption
 - B. Describe how the SSL handshake works
 - C. Describe some of the legal and security considerations related to use of the SSL proxy
- V. Managing SSL Traffic on the ProxySG**
 - A. Describe how the SSL proxy service handles SSL traffic
 - B. Describe the standard keyrings that are installed by default on the ProxySG
 - C. Identify the types of security certificates that the ProxySG uses
- VI. Optimizing SSL Interception Performance**
 - A. Configure the ProxySG to process SSL traffic according to best practices for performance
- VII. SGOS Architecture**
 - A. Identify key components of SGOS
 - B. Explain the interaction among client workers and software workers in processing client requests
 - C. Explain the significance of policy checkpoints
- VIII. Caching Architecture**
 - A. Describe the benefits of object caching on the ProxySG
 - B. Explain the caching-related steps in a ProxySG transaction
 - C. Identify and describe the HTTP request and response headers related to caching
 - D. Describe, in general terms, how the ProxySG validates cached objects to ensure freshness
 - E. Explain how the ProxySG uses cost-based deletion, popularity contests, and pipelining to improve object caching
- IX. System Diagnostics**
 - A. Describe the use of the health monitor and health checks
 - B. Explain the use of the event and access logs
 - C. Describe the information available in advanced URLs and sysinfo files
 - D. Describe the function of policy tracing and packet captures
- X. Introduction to Content Policy Language (CPL)**
 - A. Describe the fundamental concepts and purposes of ProxySG policy transactions
 - B. Understand the relationship of layers, rules, conditions, properties, and triggers
 - C. Describe the two types of actions in CPL
 - D. Describe how to write, edit, and upload CPL code
- XI. Using Policy Tracing for Troubleshooting**
 - A. Identify the two main types of ProxySG policy traces
 - B. Describe the various sections of a policy trace result
 - C. Configure a global and policy-driven trace
 - D. Access and interpret policy trace results
- XII. ProxySG Integration**
 - A. Identify other Symantec products that can be used as part of a complete security solution
- D. Describe key characteristics of the SGOS storage subsystem**
- E. Explain the caching behavior of the ProxySG**