BROADCOM®
SOFTWARE

Exam Study Guide

Exam 250-556: Symantec ProxySG 6.7 Technical Specialist

1. About Broadcom Certification Exams

Broadcom Certification demonstrates the highest levels of technical competency, productivity and industry recognition with increased opportunities for career advancement.

Validate your technical knowledge and competency by becoming a Broadcom Technical Specialistbased on your specific area of Broadcom Software technology expertise. To achieve this level of certification, candidates must pass one proctored Technical Specialistexam based on a combination of training material, commonly referenced product documentation, and real-world job scenarios.

Each certification exam is a computer-based examination that gives you the opportunity to demonstrate your mastery of critical skills sets against published exam objectives. Qualified proctors through independent test centers, on Broadcom's behalf, administer the exams. Each exam has a predefined time allowed. Please confirm timing allotted when registering for your exam. All exams are closed book, which means you may not have any printed material, computers or calculators with you during the exam. Upon completion of your exam you will receive immediate, provisional, on-screen feedback on your scoring.

For more detailed information about Broadcom Technical SpecialistExams and other Broadcom Partner certifications, please visit the Broadcom Certification Program page at https://www.broadcom.com/support/education/software/certification/all-exams

BROADCOM
SOFTWARE

2.   Preparing for Your Certification Exam

Recommended Experience

To supplement the education and training materials provided to prepare for this exam, it is recommended that the candidate has at least 3-6 months experience working with Symantec ProxySG in a production or lab environment.

Study References

<table>
<tr><td>**Instructor Led**</td><td>**https://www.broadcom.com/support/symantec/services/education**</td></tr>
</table>

ProxySG 6.7 Basic Administration (2 Day Instructor-Led or 8-Hour Self-Paced)

- Introduction to Symantec ProxySG Secure Web Gateway
  - Function of a proxy server
  - Key features and benefits of the ProxySG
- ProxySG Security Deployment Options
  - Three network deployment methods
  - Three possible roles
- ProxySG Management Console
  - Relationship between Management Console and ProxySG CLI(Lecture/Lab)
  - Primary functions of the major areas of the Management Console(Lecture/Lab)
- Traffic Interception using Proxy Services
  - Functions of proxy services, listeners,and proxy types(Lecture/Lab)
  - Intercepting and bypassing traffic(Lecture/Lab)
- Hypertext Transfer Protocol
  - Components of an HTTP URL (Lecture/Lab)
  - HTTP request and HTTP response headers (Lecture/Lab)
- Introduction to the Visual Policy Manager
  - Relationship of VPM, CPL, and Management Console (Lecture/Lab)
  - VPM objects, triggers, and actions (Lecture/Lab)
- Filtering Web Content
  - Primary category databases (Lecture/Lab)
  - How WebFilter and WebPulse work together(Lecture/Lab)
- Using Threat Intelligence to Defend the Network
  - Intelligence Services provided by the Global Intelligence Network (Lecture/Lab)
  - Using Geolocation and Threat Risk Levels in policy (Lecture/Lab)

- Ensuring Safe Downloads
    - File type detection (Lecture/Lab)
    - How malware is transmitted via HTTP (Lecture/Lab)
- Notifying Users of Internet Usage Policies
    - Built-in and custom exception pages (Lecture/Lab)
    - Coaching and splash pages (Lecture/Lab)
- Access Logging on the ProxySG
    - How access logging works on the ProxySG (Lecture/Lab)
    - Access log facility components (Lecture/Lab)
- ProxySG Initial Configuration
    - Initial configuration access methods
    - Access control

ProxySG 6.7 Advanced Administration (2 Day Instructor-Led or 8-Hour Self-Paced)

- Using Authentication Realms
    - ProxySG authentication architecture
    - Use of IWA direct and IWA BCAAA realms (Lecture/Lab)
- Understanding Authentication Credentials
    - Basic, NTLM, and Kerberos
    - Configure Kerberos authentication (Lecture/Lab)
- Understanding Authentication Modes
    - Surrogates
    - Explicit and transparent authentication (Lecture/Lab)
- Understanding HTTPS
    - Key components of SSL encryption
    - SSL handshake(Lecture/Lab)
- Managing SSL Traffic on the ProxySG
    - How the SSL proxy service handles SSL traffic(Lecture/Lab)
    - Standard keyrings and types of security certificates(Lecture/Lab)
- Optimizing SSL interception Performance
    - Best practices
- SGOS Architecture
    - Key components of SGOS
    - Policy checkpoints(Lecture/Lab)
- Caching Architecture
    - Object caching(Lecture/Lab)
    - Cost-based deletion, popularity contests, and pipelining(Lecture/Lab)
- System Diagnostics
    - Health monitor and health checks(Lecture/Lab)
    - Policy tracing and packet captures(Lecture/Lab)
- Introduction to Content Policy Language (CPL)
    - Concepts of policy transactions
    - Layers, rules, conditions, properties, and triggers(Lecture/Lab)
- Using Policy Tracing for Troubleshooting
    - Two types of policy traces(Lecture/Lab) & Policy trace sections(Lecture/Lab)

- ProxySG Integration
  - Integration with other Symantec network security solutions

ProxySG 6.7 Diagnostics and Troubleshooting (2 Day Instructor-Led or 8-Hour Self-Paced)

- ProxySG Secure Web Gateway—Diagnostics and Troubleshooting Overview
  - Review of ProxySG-based Secure Web Gateway solution
  - Common issues related to internal resources and external dependencies (Lecture/Lab)
- Exploring Sysinfo Files
  - Generating sysinfo files
  - Using sysinfo files for troubleshooting (Lecture/Lab)
- Troubleshooting Issues Related to Authentication
  - IWA direct and IWA BCAAA issues(Lecture/Lab)
  - Surrogate credentials and Schannel congestion(Lecture/Lab)
- Troubleshooting Issues Related to DNS
  - Forward and reverse DNS lookups(Lecture/Lab)
  - DNS imputing issues(Lecture/Lab)
- Troubleshooting SSL Interception Issues
  - Diagnosing SSL interception issues(Lecture/Lab)
  - Connection and performance issues(Lecture/Lab)
- Troubleshooting Performance Issues Related to Policy Efficiency
  - Optimizing performance

Documentation   **https://support.broadcom.com/**

- **SGOS Administration Guide (6.7x)**
- **Configure the SWG VA**
- **Proxy SG Security Best Practices**

Broadcom Websites

- **Symantec ProxySG Landing Page**

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the exam and how these objectivesalign to the corresponding Symantec course topics and their associated lab exercises as well as the referenced product documentation.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.For more information on the Broadcom Certification Program, visit **https://www.broadcom.com/support/symantec/services/education/certification**.

Introduction to the Symantec ProxySG Secure Web Gateway

Exam Objectives	Applicable Course Content
Describe the functions of a proxy server	
Differentiate proxy servers from firewalls	**Symantec ProxySG 6.7 Basic Administration**
Describe the key features and benefits of the Symantec ProxySG	• Module: Introduction to the Symantec ProxySG Secure Web Gateway
List the various ProxySG models	
Access online Symantec community resources	

ProxySG Security Deployment Options

Exam Objectives	Applicable Course Content
Describe the three network deployment options	**Symantec ProxySG 6.7 Basic Administration**
Describe the three possible roles of the ProxySG	• Module: ProxySG Security Deployment Options

ProxySG Management Console

Exam Objectives	Applicable Course Content
Describe the relationship between the Management Console and the ProxySG CLI	**Symantec ProxySG 6.7 Basic Administration** • Module: ProxySG Management Console
Describe the primary function of the major areas ofthe Management Console	
Use the Management Console to access on-boxhelp and Symantec product documentation	

Traffic Interception using Proxy Services

Exam Objectives	Applicable Course Content
Understand the functions of proxy services,listeners, and proxy types	**Symantec ProxySG 6.7 Basic Administration** • Module: Traffic Interception using Proxy Services
Describe the three most common proxy services	
Explain how the intercept and bypass settings affect what happens to network traffic passingthrough the ProxySG	

Hypertext Transfer Protocol

Exam Objectives	Applicable Course Content
Understand how a connection is initiated over thetransport layer	**Symantec ProxySG 6.7 Basic Administration** • Module: Hypertext Transfer Protocol
Identify the components of an HTTP URL	
Explain the two types of HTTP messages: requestand response	

Introduction to the Visual Policy Manager

Exam Objectives	Applicable Course Content
Describe the relationship among the VPM, CPL, andthe Management Console	**Symantec ProxySG 6.7 Basic Administration** • Module: Introduction to the Visual Policy Manager
Describe the default processing order for policylayers and rules	
Describe triggers and actions that can be used inwriting policy	

Filtering Web Content

Exam Objectives	Applicable Course Content
Describe the main concepts of web filtering	**Symantec ProxySG 6.7 Basic Administration** • Module: Filtering Web Content
Describe the primary category databases	
Describe the category types available to policy	
Describe how Blue Coat WebFilter and WebPulsework together	

Using Threat Intelligence to Defend the Network

Exam Objectives	Applicable Course Content
Understand Intelligence Services as provided bythe Global Intelligence Network	**Symantec ProxySG 6.7 Basic Administration** • Module: Using Threat Intelligence to Defend the Network
Understand Geolocation and Threat Risk Levels andhow they can be used in policy	

Ensuring Safe Downloads

Exam Objectives	Applicable Course Content
Describe how malware can be transmitted viaHTTP	**Symantec ProxySG 6.7 Basic Administration** • Module: Ensuring Safe Downloads
Explain the methods, advantages, anddisadvantages of file type detection	
Describe some of the considerations in deciding what content to block as possible malware sources	

Notifying Users of Internet Usage Policies

Exam Objectives	Applicable Course Content
Explain the function and various components ofbuilt-in and custom exception pages	**Symantec ProxySG 6.7 Basic Administration** • Module: Notifying Users of Internet Usage Policies
Describe the function of Notify User objects	
Identify the types of pages that can be sent tousers by using Notify User objects	
Describe splash pages and coaching pages usingNotify User objects in the VPM	

Access Logging on the ProxySG

Exam Objectives	Applicable Course Content
Describe, at a high level, how the ProxySGperforms access logging	**Symantec ProxySG 6.7 Basic Administration** • Module: Access Logging on the ProxySG
Describe the components of a ProxySG access logfacility	
Identify default log facilities and log formats	
Describe common use cases for periodic andcontinuous uploading of access logs	

ProxySG Initial Configuration

Exam Objectives	Applicable Course Content
Access the ProxySG and perform initial configuration	**Symantec ProxySG 6.7 Basic Administration** • Appendix A: ProxySG Initial Configuration
Describe the two SGOS editions and various license types	
Understand the optional capabilities available with SGOS	

Using Authentication Realms

Exam Objectives	Applicable Course Content
Describe the benefits of enabling authentication onthe ProxySG	**Symantec ProxySG 6.7 Advanced Administration** • Module: Using Authentication Realms
Describe, at a high level, the ProxySGauthentication architecture	
Understand the use of IWA realms, with both IWADirect and IWA BCAAA connection methods	

Understanding Authentication Credentials

Exam Objectives	Applicable Course Content
Describe how NTLM and Kerberos authenticationwork in both IWA direct and IWA BCAAA deployments	**Symantec ProxySG 6.7 Advanced Administration** • Module: Understanding Authentication Credentials
Configure the ProxySG to use Kerberosauthentication	

Understanding Authentication Modes

Exam Objectives	Applicable Course Content
Describe authentication surrogates andauthentication modes	**Symantec ProxySG 6.7 Advanced Administration** • Module: Understanding Authentication Modes
Describe ProxySG authentication in both explicitand transparent deployment mode	

Understanding HTTPS

Exam Objectives	Applicable Course Content
Describe authentication surrogates andauthentication modes	**Symantec ProxySG 6.7 Advanced Administration** • Module: Understanding HTTPS
Describe ProxySG authentication in both explicitand transparent deployment mode	

Managing SSL Traffic on the ProxySG

Exam Objectives	Applicable Course Content
Describe how the SSL proxy service handles SSLtraffic	**Symantec ProxySG 6.7 Advanced Administration** • Module: Managing SSL Traffic on the ProxySG
Describe the standard keyrings that are installed bydefault on the ProxySG	
Identify the types of security certificates that theProxySG uses	

Optimizing SSL Interception Performance

Exam Objectives	Applicable Course Content
Configure the ProxySG to process SSL trafficaccording to best practices for performance	**Symantec ProxySG 6.7 Advanced Administration** • Module: Optimizing SSL Interception Performance

SGOS Architecture

Exam Objectives	Applicable Course Content
Identify key components of SGOS	**Symantec ProxySG 6.7 Advanced Administration** • Module: SGOS Architecture
Explain the interaction among client workers andsoftware workers in processing client requests	
Explain the significance of policy checkpoints	

Caching Architecture

Exam Objectives	Applicable Course Content
Describe the benefits of object caching on theProxySG.	**Symantec ProxySG 6.7 Advanced Administration** • Module: Caching Architecture
Explain the caching-related steps in a ProxySGtransaction.	
Identify and describe the HTTP request andresponse headers related to caching.	

System Diagnostics on the ProxySG

Exam Objectives	Applicable Course Content
Describe the use of the health monitor and healthchecks	
Explain the use of the event and access logs	**Symantec ProxySG 6.7 Advanced Administration**
Describe the information available in advanced URLs and sysinfo files	• Module: System Diagnostics on the ProxySG
Describe the function of policy tracing and packetcaptures	

Introduction to CPL

Exam Objectives	Applicable Course Content
Describe the fundamental concepts and purposesof ProxySG policy transactions	
Understand the relationship of layers, rules,conditions, properties, and triggers	**Symantec ProxySG 6.7 Advanced Administration** • Module: Introduction to CPL
Describe the two types of actions in CPL	

Using Policy Tracing for Troubleshooting

Exam Objectives	Applicable Course Content
Identify the two main types of ProxySG policytraces	**Symantec ProxySG 6.7 Advanced Administration** • Module: Using Policy Tracing for Troubleshooting
Describe the various sections of a policy traceresult	
Configure a global and policy-driven trace	
Access and interpret policy trace results	

ProxySG Integration

Exam Objectives	Applicable Course Content
Identify other Symantec products that can be usedas part of a complete security solution	**Symantec ProxySG 6.7 Advanced Administration** • Module: ProxySG Integration

Symantec ProxySG Secure Web Gateway—Diagnostics and Troubleshooting Overview

Exam Objectives	Applicable Course Content
Provide an overview of the ProxySG Secure WebGateway Solution functions and components	
Provide an overview of ways you can monitor CPUusage on the ProxySG	
Provide an overview of ways you can monitormemory usage on the ProxySG	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Symantec ProxySG Secure Web Gateway—Diagnostics and Troubleshooting Overview
Provide an overview of ways you can monitorbandwidth usage on the ProxySG	
Understand the relationship with external dependencies such as DNS and ICAP servers	
Provide an overview of SSL interception issues onthe ProxySG	

Exploring Sysinfo Files

Exam Objectives	Applicable Course Content
Understand the components of a sysinfo file	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Exploring Sysinfo Files
Understand the various sections of a sysinfo file	

Troubleshooting Issues Related to Authentication

Exam Objectives	Applicable Course Content
Description of components, architecture, and process flow of authentication	
Define issues related to authentication	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Troubleshooting Issues Related to Authentication
Diagnose issues related to authentication	
Solve issues related to authentication	
Communicate results	

Troubleshooting Issues Related to DNS

Exam Objectives	Applicable Course Content
Description of components, architecture, and process flow of authentication	
Define issues related to authentication	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Troubleshooting Issues Related to DNS
Diagnose issues related to authentication	
Solve issues related to authentication	
Communicate results	

Troubleshooting SSL Interception Issues

Exam Objectives	Applicable Course Content
Description of components, architecture, and process flow of authentication	
Define issues related to authentication	
Diagnose issues related to authentication	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Troubleshooting SSL Interception Issues
Solve issues related to authentication	
Communicate results	

Troubleshooting Performance Issues related to policy efficiency

Exam Objectives	Applicable Course Content
Description of components, architecture, and process flow of authentication	
Define issues related to authentication	
Diagnose issues related to authentication	**Symantec ProxySG 6.7 Diagnostics and Troubleshooting** • Module: Troubleshooting Performance Issues related to policy efficiency
Solve issues related to authentication	
Communicate results	

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. **Where can an administrator find links to resources such as instructional CBTs, technical webcasts, and knowledge base articles?**

   A. Symantec Enterprise Technical Support
   B. Customer forums
   C. ProxySG First Steps WebGuide
   D. Symantec Blue Coat YouTube channel

2. **Which is the advantage of an inline deployment?**

   A. Ease of deployment
   B. More easily implement redundancy
   C. Narrowing the amount of traffic to the ProxySG
   D. Eliminates single point of failure

3. **Which defines the ports on which the ProxySG listens for incoming requests?**

   A. Policies
   B. SGOS version
   C. Services
   D. Subscription licenses

4. **Which two (2) options allow an administrator to create policy? (Select two)**

   A. In the Visual Policy Manager
   B. Directly in Content Policy Language
   C. From Proxy services
   D. In the CLI
   E. In the initial configuration

5. **Which two (2) components are necessary to filter web content? (Select two)**

   A. Content filtering database
   B. SSL Proxy services
   C. Configured policy
   D. Local database
   E. A third-party filtering application

6. **What allows Symantec to dynamically analyze and categorize new web content?**

    A. Geolocation
    B. Threat risk levels
    C. Application filtering
    D. Global Intelligence Network

7. **Which two (2) protocols can an administrator use to upload access logs? (Select two)**

    A. HTTP
    B. ICAP
    C. FTP
    D. WCCP
    E. IMAP

8. **Which provides visibility into who is going where on the network?**

    A. Authorization on the ProxySG
    B. Authentication on the ProxySG
    C. Certificate validation
    D. The event log

9. **Which provides an encrypted tunnel through which other protocols can pass?**

    A. HTTP
    B. Certificate authorities
    C. Secure Socket Layer
    D. PKI

10. **Over which protocol does the ProxySG communicate with virus scanning appliances?**

    A. HTTP
    B. HTTPS
    C. FTP
    D. ICAP

11. **Where can you also find most of the information contained in a sysinfo file?**

    A. Help files on the ProxySG
    B. Symantec technical support webpage
    C. Advanced URLs on the ProxySG
    D. Event logs

12. **Which is the first section displayed in a sysinfo file?**

    A.   System, version, and hardware information
    B.   Health check statistics
    C.   Configured policy
    D.   Event log

13. **Which advanced URL allows you to look at specific DNS servers added to the ProxySG?**

    A.   /tcp/dns-ns-stats
    B.   /tcp/dns-query-stats
    C.   /dns
    D.   /dns/tcp-ns-stats

14. **What enables HTTP caching to be applied to HTTPS content?**

    A.   SSL traffic interception
    B.   Disabling authentication
    C.   SSL traffic tunneling
    D.   Disabling Detect Protocol

15. **From where do ProxySG administrators issue web requests?**

    A.   From the Management Console
    B.   From a browser
    C.   From a Java applet
    D.   From the Visual Policy Manager

Sample Exam Answers:

1. A, B
2. A
3. C
4. A, B
5. A, C
6. D
7. A, C
8. B
9. C
10. D
11. C
12. A
13. A
14. A
15. B