Exam Study Guide

ProxySG 7.3 Administration with Secure Web Gateway

EXAM CODE: 250-557

Exam Description

Candidates can validate technical knowledge and competency by becoming a Symantec Certified Specialist (SCS) based on your specific area of Broadcom Software technology expertise. To achieve this level of certification, candidates must pass this proctored SCS exam that is based on a combination of Broadcom Software training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the ProxySG and related Secure Web Gateway products in a Security Operations role. This certification exam tests the candidate's knowledge on how to administer the ProxySG and related products including SSL Visibility Appliance, Content Analysis, Management Center, Reporter, and Web Isolation.

For more information about Broadcom Software's certification program, see

https://www.broadcom.com/support/education/software/certification

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with the ProxySG and related SWG products in a production or lab environment.

Study References

Courses

ProxySG 7.3 Administration with Secure Web Gateway (4 days Instructor-Led)

- Introduction to the Secure Web Gateway
  - The need for a secure web gateway
  - Introduction to the ProxySG
  - ProxySG deployment options
  - Introduction to related Symantec SWG products
- Intercepting traffic and applying policy
  - How the ProxySG intercepts traffic
  - Write policy on the ProxySG
  - Layer and rule evaluation on the ProxySG
- Apply security and web usage policy to encrypted traffic
  - Introduction to TLS encryption
  - Manage HTTPS traffic on the ProxySG
  - Integrate the SSL Visibility Appliance
- Provide security and web usage policies based on role or group
  - Introduction to role-based access control
  - Authentication basics on the ProxySG
  - Use an IWA authentication realm
  - Authentication modes
  - Using IWA direct and IWA BCAAA
  - Use roles and groups in policy
- Enforce corporate guidelines for acceptable Internet browsing behavior
  - Write appropriate internet use policies
  - Notify users of internet usage policies
- Protect the endpoint from malicious activity
  - WebPulse technical details
  - Introduction to Intelligence Services
  - Use Threat Intelligence to defend the network
  - Ensure safe downloads
- Centrally manage, monitor, and report on security activity
  - Introduction to Management Center
  - Integrate Management Center with the Secure Web Gateway
  - Introduction to Symantec Reporter
  - Configure access logging on the ProxySG
  - Preparing Reporter to receive ProxySG access logs
- Maintain the ProxySG, Management Center, and Reporter
  - Monitoring the ProxySG within Management Center
  - Administering Management Center and Reporter
- Prevent malware and phishing threats while allowing broad web access
  - Symantec Web Isolation overview
  - Provide selective or full web isolation
  - Protect against phishing attacks
  - Integration with other security solutions

- Enhance security by adding virus scanning, sandboxing, and data loss prevention
  - Virus scanning and sandboxing with Content Analysis
  - Communication over ICAP
  - Protect sensitive data with Symantec Data Loss Prevention
- Expand security capabilities with cloud integrations
  - Introduction to Web Security Service
  - Using Universal Policy Enforcement
  - Integrate CloudSOC with the Secure Web Gateway

Documentation

- ProxySG 7.1
  - SGOS Administration Guide 7.3.x
  - SGOS Upgrade/Downgrade Guide
  - ProxySG Reverse Proxy Deployment Guide
  - ProxySG 7.3.x Security Best Practices
- https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-1/admin-guide.html

Website

- https://www.broadcom.com/support/education/software/training-courses
- https://www.broadcom.com/support/education/symantec/elibrary
- https://www.broadcom.com/products/cyber-security/web-and-email

Exam Objectives

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

It is strongly recommended that all candidates complete all applicable lab exercises in preparation for the exam.

Introduction to the Secure Web Gateway

Exam Objectives	Applicable Course Content
Understand the need for a secure web gateway solution	**ProxySG 7.3 Administration with SWG** Module: Introduction to the Secure Web Gateway
Describe the basic features and functions of the ProxySG and other Secure Web Gateway products	
Understand ProxySG deployment options	

Interception traffic and applying policy

Exam Objectives	Applicable Course Content
Understand how the ProxySG intercepts traffic	**ProxySG 7.3 Administration with SWG** Module: Apply security and web usage policy to encrypted traffic
Learn how to write policy on the ProxySG	
Understand layer and rule evaluation order in the VPM	

Apply security and web usage policy to encrypted traffic

Exam Objectives	Applicable Course Content
Describe the basics of TSL encryption	**ProxySG 7.3 Administration with SWG** Module: Apply security and web usage policy to encrypted traffic
Describe how HTTPS traffic is managed on the ProxySG	
Describe how the SSL Visibility Appliance can be integrated with the ProxySG	

Provide security and web usage policies based on role or group

Exam Objectives	Applicable Course Content
Describe how authentication on the ProxySG is handled	**ProxySG 7.3 Administration with SWG** Module: Provide security and web usage policies based on role or group
Understand how IWA authentication realms work	
Describe how authentication modes work	
Using IWA Direct and IWA BCAAA	

Enforce corporate guidelines for acceptable Internet browsing behavior

Exam Objectives	Applicable Course Content
Understand how to write appropriate Internet usage policies	**ProxySG 7.3 Administration with SWG** Module: Enforce corporate guidelines for acceptable Internet browsing behavior
Describe how to notify users of Internet usage policies	

Protect the endpoint from malicious activity

Exam Objectives	Applicable Course Content
Understand how to use Threat Intelligence to defend the network	**ProxySG 7.3 Administration with SWG** Module: Protect the endpoint from malicious activity
Describe how to ensure safe downloads	

Centrally manage, monitor, and report on security activity

Exam Objectives	Applicable Course Content
Understand how Management Center works	**ProxySG 7.3 Administration with SWG** Module: Centrally manage, monitor, and report on security activity
Understand how Reporter works	
Describe how to integrate the ProxySG and Reporter with Management Center	

Maintain the ProxySG, Management Center and Reporter for optimal performance

Exam Objectives	Applicable Course Content
Monitor the ProxySG from within Management Center	**ProxySG 7.3 Administration with SWG** Module: Maintain the ProxySG, Management Center, and Reporter
Administer Management Center	
Administer Reporter	

Prevent malware and phishing threats while allowing broad web access

Exam Objectives	Applicable Course Content
Describe how Web Isolation works	**ProxySG 7.3 Administration with SWG** Module: Prevent malware and phishing threats while allowing broad web access
Understand how to prevent phishing attacks	
Describe how Web Isolation can be integrated with other solutions	

Enhance security by adding virus scanning, sandboxing, and data loss prevention

Exam Objectives	Applicable Course Content
Understand how the Content Analysis performs virus scanning and sandboxing	**ProxySG 7.3 Administration with SWG** Module: Enhance security by adding virus scanning, sandboxing, and data loss prevention
Understand how communication over ICAP works	
Describe how Content Analysis can be integrated with the ProxySG and with Symantec Data Loss Prevention	

Expand security capabilities with cloud integrations

Exam Objectives	Applicable Course Content
Understand how Web Security Service (WSS) can be integrated into the SWG solution	**ProxySG 7.3 Administration with SWG** Module: Expand security capabilities with cloud integrations
Understand how CloudSOC can be integrated into the SWG solution	

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 two (2) categories of HTTPS traffic are typically not decrypted? (Select two)

A. Financial services
B. Health
C. Social media
D. News media E. Gambling

3. Which threat risk level would likely be assigned to an unproven URL without an established history of normal behavior?

A. Low
B. Medium-Low
C. Medium
D. High

4. Which protocol does the ProxySG use to communicate with Symantec DLP?

A. Secure Socket Layer
B. File Transfer Protocol
C. Hypertext Transport Protocol
D. Internet Content Adaption Protocol

5. How would an administrator restrict the ability of financial personnel to access HR records in Reporter?

A. Configure separate databases for financial and HR records
B. Restrict access by financial personnel to HR-related fields in the database
C. Ensure that HR log sources are not uploaded to financial databases
D. Assign dedicated ProxySGs for each assigned role in the company

Sample Exam Answers

1. A
2. A, B
3. C
4. C
5. C