BROADCOM

250-589: Symantec Web Protection— Edge SWG R2 Technical Specialist

Exam Study Guide

Exam Description

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

This exam targets IT Professionals using Edge SWG products in a Security Operations role. This certification exam tests the candidate's knowledge on how to administer Edge SWG features including Edge SWG, Content Analysis, Management Center, Reporter, and High Risk Isolation; as well as diagnose and troubleshoot common issues related to Edge SWG deployments.

Recommended Experience

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

Study References

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

Symantec Web Protection—Edge SWG Administration R2 (3-Day Instructor- led)

- Introduction to Symantec Edge SWG
- Intercepting traffic and applying policy
- Applying security and web usage policy to encrypted traffic
- Centrally managing devices with Management Center
- Providing security and web usage policies based on role or group
- Enforcing corporate guidelines for acceptable Internet browsing behavior
- Protecting the endpoint from malicious activity
- Providing security for risky and unknown websites with High Risk Isolation
- Enhancing security with virus scanning
- Using malware analysis to analyze potentially malicious files
- Monitoring Edge SWG features
- Reporting for Edge SWG features
- Understanding SGOS architecture and caching on Edge SWG
- Using built-in diagnostic tools on Edge SWG
- Expanding security with cloud integrations

Instructor

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

Symantec Web Protection—Edge SWG Diagnostics & Troubleshooting R2 (1-Day Instructor-led)

- Edge SWG diagnostics and troubleshooting overview
- Diagnosing common issue on Edge SWG
- Troubleshooting authentication issues on Edge SWG
- Troubleshooting encrypted traffic management issues on Edge SWG
- Troubleshooting DNS issues on Edge SWG
- Troubleshooting Policy issues on Edge SWG

Documentati

https://techdocs.broadcom.co

Edge SWG
- SGOS Administration Guide
- SGOS Upgrade/Downgrade Guide
- Edge SWG 7.3.x Security Best Practices

Symantec Websites

- Network Security Landing Page

Exam Topics

The following tables list some areas to be familiar with, organized by course module, in preparation for taking the Symantec Certification exam.

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/education/software/certification

https://www.broadcom.com/support/education/software/certification/all-exams

Introduction to Symantec Edge SWG

Exam Topics	Applicable Course Content
• Symantec Web Protection overview • Introduction to Edge SWG • Key Edge SWG use cases	**Edge SWG Administration R2** Module 1: Introduction to Symantec Edge SWG

Intercepting traffic and applying policy

Exam Topics	Applicable Course Content
• How Edge SWG intercepts traffic • Writing Edge SWG policy in the Visual Policy Manager • Informing users when web access is denied or restricted due to policy	**Edge SWG Administration R2** Module 2: Intercepting traffic and applying policy

Applying security and web usage policy to encrypted traffic

Exam Topics	Applicable Course Content
• Introduction to TLS encryption • Managing HTTPS traffic on Edge SWG • Offloading HTTPS traffic to the SSL Visibility Appliance to boost performance	**Edge SWG Administration R2** Module 3: Applying security and web usage policy to encrypted traffic

Centrally managing devices with Management Center

Exam Topics	Applicable Course Content
• How Management Center centralizes and simplifies Edge SWG management • Configuring Edge SWG with the SG Admin Console • Creating and distributing VPM policies • Creating and managing jobs	**Edge SWG Administration R2** Module 4: Centrally managing devices with Management Center

Providing security and web usage policies based on role or group

Exam Topics	Applicable Course Content
• Authentication basics on Edge SWG • Using IWA authentication on Edge SWG • Authentication modes in explicit and transparent proxy deployments • Connecting to the Windows domain directly using IWA direct • Connecting to the Windows domain using IWA BCAAA • Introduction to role-based access control • Using roles and groups in policy	**Edge SWG Administration R2** Module 5: Providing security and web usage policies based on role or group

Enforcing corporate guidelines for acceptable Internet browsing behavior

Exam Topics	Applicable Course Content
• Creating strong corporate guidelines for acceptable Internet use • Using website categorization to enforce acceptable use guidelines • Providing Edge SWG with categorization databases to be referenced in policy • Setting the Request URL Category object in policy to enforce acceptable use guidelines • Applying policy in order to enforce acceptable use guidelines	**Edge SWG Administration R2** Module 6: Enforcing corporate guidelines for acceptable Internet browsing behavior

Protecting the endpoint from malicious activity

Exam Topics	Applicable Course Content
• Requirements for a pre-emptive, layered web defense • WebPulse technical details • Introduction to Intelligence Services • Using Intelligence Services data feeds in policy • Ensuring safe downloads • Combined policy example	**Edge SWG Administration R2** Module 7: Protecting the endpoint from malicious activity

Providing security for risky and unknown for risky and unknown websites with HRI

Exam Topics	Applicable Course Content
• Instroduction to High Risk Isolation? • Configuring HRI • Overview of Full Isolation	**Edge SWG Administration R2** Module 8: Providing security for risky and unknown for risky and unknown websites with High Risk Isolation

Enhancing security with virus scanning

Exam Topics	Applicable Course Content
• Introduction to Content Analysis • Configuring communication with Edge SWG over ICAP • Configure malware scanning options on Edge SWG	**Edge SWG Administration R2** Module 9: Enhancing security and virus scanning

Using Malware Analysis to analyze potentially malicious files

Exam Topics	Applicable Course Content
• Introduction to Malware Analysis • Preparing to use Malware Analysis • Performing Malware Analysis	**Edge SWG Administration R2** Module 10: Using malware analysis to analyze potentially malicious files

Monitoring Edge SWG features

Exam Topics	Applicable Course Content
• Monitoring devices from within Management Center • Configuring device alerts in Management Center • Using Active Sessions and the Event Log on Edge SWG • Using health checks on Edge SWG • Monitoring Content Analysis • Monitoring Reporter	**Edge SWG Administration R2** Module 11: Monitoring Edge SWG features

Reporting for Edge SWG features

Exam Topics	Applicable Course Content
• How Reporter delivers centralizeed web reporting and visibility • Configuring access logging on Edge SWG to integrate with Reporter • Using the RPAC to configure log processing on Reporter • Running reports •	**Edge SWG Administration R2** Module 12: Reporting for Edge SWG features

Understanding SGOS architecture and caching on Edge SWG

Exam Topics	Applicable Course Content
• SGOS architecture • Caching on Edge SWG • Using HTTP compression	**Edge SWG Administration R2** Module 13: Understanding SGOS architecture and caching on Edge SWG

Using built-in diagnostic tools on Edge SWG

Exam Topics	Applicable Course Content
• Exploring sysinfo files • Using policy tracing and policy coverage tools to analyze policy decisions • Using packet captures to analyze network traffic • Sending service information to Symantec support	**Edge SWG Administration R2** Module 14: Using built-in diagnostic tools on Edge SWG

Expanding security with cloud integrations

Exam Topics	Applicable Course Content
• Introduction to Cloud SWG • Using Universal Policy Enforcement • Integrating CloudSOC with Symantec Network Protection	**Edge SWG Administration R2** Module 15: Expanding security with cloud integrations

Edge SWG diagnostics and troubleshooting overview

Exam Topics	Applicable Course Content
• Symantec troubleshooting methodology • Symantec Edge SWG component review • Key diagnostic tools review	**Edge SWG Diagnostics and Troubleshooting R2** Module 1: Edge SWG diagnostics and troulbeshooting overview

Diagnosing common issues on Edge SWG

Exam Topics	Applicable Course Content
• Diagnosing CPU usage issues • Diagnosing memory usage issues • Diagnosing issues with external dependencies	**Edge SWG Diagnostics and Troubleshooting R2** Module 2: Diagnosing common issues on Edge SWG

Troubleshooting authentication issues on Edge SWG

Exam Topics	Applicable Course Content
• Overview of authentication on Edge SWG • Defining issues related to authentication • Diagnosing issues related to authentication • Solving issues related to authentication • Result—Communicating result or contacting Symantec support	**Edge SWG Diagnostics and Troubleshooting R2** Module 3: Troubleshooting authentication issues on Edge SWG

Troubleshooting encrypted traffic management issues on Edge SWG

Exam Topics	Applicable Course Content
• Review of SSL interception on Edge SWG • Defining issues related to SSL interception • Diagnosing issues related to SSL interception • Solving issues related to SSL interception • Result—Communicating result or contacting Symantec support	**Edge SWG Diagnostics and Troubleshooting R2** Module 4: Troubleshooting encrypted traffic management issues on Edge SWG

Troubleshooting DNS issues on Edge SWG

Exam Topics	Applicable Course Content
• Overview of DNS service on Edge SWG • Defining issues related to DNS lookups • Diagnosing issues related to DNS lookups • Solving issues related to DNS lookups • Result—Communicating result or contacting Symantec support	**Edge SWG Diagnostics and Troubleshooting R2** Module 5: Troubleshooting DNS issues on Edge SWG

Troubleshooting policy issues on Edge SWG

Exam Topics	Applicable Course Content
• Review of policy operation on Edge SWG • Defining policy issues on Edge SWG • Diagnosing policy issues on Edge SWG • Solving policy issues on Edge SWG • Result—Communicating result or contacting Symantec support	**Edge SWG Diagnostics and Troubleshooting R2** Module 6: Troubleshooting policy issues on Edge SWG

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. Which is the primary advantage of an inline Edge SWG deployment?
   A. Ease of deployment
   B. More easily implemented redundancy
   C. Decreases the amount of traffic to Edge SWG
   D. Eliminates single point of failure
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 Edge SWG 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 Edge SWGs for each assigned role in the company

Sample Exam Answers:

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