Exam Study Guide

Administration of Symantec Secure Sockets Layer Visibility 5.0

EXAM CODE: 250-444

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 the Symantec Secure Sockets Layer Visibility product in a Security Operations role. This certification exam tests the candidate's knowledge on how to how to install, configure and administer Symantec Security Analytics.

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 Symantec Secure Sockets Layer Visibility (SSLV) in a production or lab environment.

Study References

Instructor

https://www.broadcom.com/support/symantec/services/edu

SSL Visibility 5.0 Administration (2 Day Instructor-Led or 8-Hour Self-Paced)

- Introduction to Traffic Management
- Introduction to SSLV Virtual Appliance
- Encrypted Traffic Management with SSL
- Deploying the SSL Visibility Appliance
- Migrating and Upgrading the SSLV
- Exposing Encrypted Inbound SSL Traffic
- Exposing Encrypted Outbound SSL Traffic
- Expose Encrypted Threats for Forensic Analysis While Complying with Privacy Regulations
- Offloading SSL Decryption for ProxySG Efficiency
- Simplify Management of Multiple SSLV Appliances with Management Center

Documentati

https://support.broadcom.com/sec

- SSLV Documentation <Link>

Symantec Websites

- Symantec SSL Visibility Landing Page

Exam Objectives

The following tables list the Broadcom 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.

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/all-exams

Introduction to Encrypted Traffic Management

Exam Objectives	Applicable Course Content
Understand SSL/TLS: History and purpose of SSL/TLS Basic components of a SSL/TLS connection Risks and benefits of SSL/TLS encryption Public Key Infrastructure and Certificates Encryption Traffic Management and SSL/TLS inspection techniques	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Introduction to Encrypted Traffic Management

Introduction to SSLV Virtual Appliance

Exam Objectives	Applicable Course Content
Describe the purpose and function of the SSLV Virtual Appliance	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Introduction to SSLV Virtual Appliance
Describe the SSLV Virtual Appliance Deployment Modes	
Perform a setup of a SSLV Virtual Appliance	

Introducing Encrypted Traffic Management with SSL

Exam Objectives	Applicable Course Content
Describe SSLV decryption techniques	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Introducing Encrypted Traffic Management with SSL
Describe SSLV hardware and understand how it is deployed	
Provide an overview of the SSLV WEbUI	
Describe SSLV access and management control	

Deploying the SSL Visibility Appliance

Exam Objectives	Applicable Course Content
Determine the best deployment options for a network environment and attached security device.	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Deploying the SSL Visibility Appliance
Understand the initial physical connections, setup script and license installation.	
Implement the SSLV in the most common configurations for forwarding and decrypting interesting SSL flows to security devices for analysis.	

Migrating and Upgrading the SSLV

Exam Objectives	Applicable Course Content
Ability to perform the following migrations: Migrating SSLV 3.9 to 4.3 Migrating SSLV 4.2 to 4.3	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Migrating and Upgrading the SSLV

Exposing Encrypted Inbound SSL Traffic

Exam Objectives	Applicable Course Content
Determine the topology requirements to install the SSLV in the proposed environment.	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Exposing Encrypted Inbound SSL Traffic
Understand the physical connection requirements for each failure mode.	
Implement the SSLV in for inline active decryption of inbound SSL	
.Understand the copy port use for passive security devices.	
Monitor the disposition of SSL flows through the SSLV	

Exposing Encrypted Outbound SSL Traffic

Exam Objectives	Applicable Course Content
Determine the topology requirements to install the SSLV in the proposed environment.	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Exposing Encrypted Outbound SSL Traffic
Understand the physical connection requirements for each failure mode.	
Implement the SSLV in for inline active decryption of inbound SSL	
.Understand the copy port use for passive security devices.	
Monitor the disposition of SSL flows through the SSLV	

Exposing Encrypted Threats for Forensic Analysis While Complyingwith Privacy Regulations

Exam Objectives	Applicable Course Content
Describe international privacy laws and regulation and their impact on exposing encrypted traffic	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Exposing Encrypted Threats for Forensic Analysis While Complying with Privacy Regulations
Describe SSLV Host Categorization and how to implement it	

Offloading SSL Decryption for ProxySG Efficiency

Exam Objectives	Applicable Course Content
Determine the topology requirements to install the SSLV in this environment.	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Offloading SSL Decryption for ProxySG Efficiency
Understand the physical connection requirements for the failure mode.	
Configure the SSLV for inline active decryption of outbound SSL traffic, with forwarding of clear text data to the attached ProxySG.	
Understand the copy port use for passive security devices.	
Configure the ProxySG for SSL offload to the SSLV.	
Monitor the disposition of SSL flows through the SSLV.	

Simplify Management of Multiple SSLV Appliances with Management Center

Exam Objectives	Applicable Course Content
Manage multiple SSLV appliances with Management Center	**Administration of Symantec Secure Sockets Layer Visibility 5.0 Course** • Module: Offloading SSL Decryption for ProxySG Efficiency
Manage SSLV lists with Management Center	
Use Management Center to handle SSLV upgrades for multiple SSLV appliances	

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. **Why have the versions of SSL and TLS changed over time?**

   A. To identify new certificate authorities
   B. To add more hosts to the encryption policy
   C. To implement better security measures
   D. To enforce data integrity

2. **Which two (2) pieces of information are contained in the server's response to the client's request, when an SSL/TLS session is initiated? (Select two)**

   A. Server certificate
   B. Server public key
   C. Server private key
   D. Client public key
   E. Client private key

3. **Which connectivity mode sends SSL traffic to the inspecting device and the inspecting device returnsit to the SSLV after processing?**

   A. Active-Inline
   B. Passive-Inline
   C. Active-tap
   D. Passive-tap

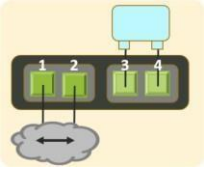
4. **Which is a grouping of interfaces that receives a network feed and enforces policy?**

   A. Ruleset
   B. Policy list
   C. Segment
   D. Aggregation port

5. **What is the job of the Inspection Services?**

   A. It defines how the traffic is to be inspected
   B. It allows SSL/TLS flows to be logged
   C. It defines what traffic is to be inspected
   D. It tracks flows that have been proxied

6. **Refer to the exhibit. What action will take place for traffic on the wire, if a failure takes place?**



A. Traffic will Fail, dropping completely not be inspected by the security device
B. Traffic will Fail-to-Appliance and continue to pass not decrypted but still inspected
C. Traffic will not Fail at all, continue to be decrypted and inspected by the security device
D. Traffic will Fail-to-Network and continue to pass not decrypted and uninspected

7. **How are the management ports paired on failure, for appliances with more than one managementinterface?**

A. Management port 1 is port paired with management port 2
B. Management ports are not paired, only network ports are
C. Management port 1 is paired with network port 1 and so on
D. Management port 1 is paired with the last network port

8. **What does the term “fail-to-appliance” refer to?**

A. It means that network traffic is sent to the SSLV appliance on physical failure
B. It means that management traffic is sent to the redundant appliance on failure
C. It means that traffic is no longer sent to the active security appliance on failure
D. It means that network traffic is sent to the active security appliance on failure

9. **What is the minimal number of copy ports that must be used to send directional (from side A or side B) traffic from the network ports to the copy port(s)?**

A. Only One
B. Two or more
C. Two or Four
D. All Four

10. **Why would the first policy push, to the SSLV from the Management Center, present a warningmessage?**

A. The existing policy is about to be overwritten
B. To warn the administrator of a policy change
C. The appliance contains the wrong device ID
D. The policy is going to the wrong type of device

Sample Exam Answers:

1. C
2. A and B
3. A
4. C
5. A
6. D
7. B
8. D
9. B
10. A