

Exam : 250-589

Title : Symantec Web Protection -
Edge SWG R2 Technical
Specialist

Version : DEMO

1.Which log should be checked when troubleshooting policy enforcement issues in Edge SWG?

- A. Event Log
- B. SSL Certificate Log
- C. Firewall Traffic Log
- D. Bandwidth Utilization Log

Answer: A

2.Which authentication settings can be configured in Edge SWG to ensure secure role-based policy enforcement? (Select two)

- A. Enabling group-based authentication rules
- B. Restricting access based on job function and department
- C. Allowing anonymous browsing for all users
- D. Bypassing authentication for social media websites

Answer: AB

3.Which two categories of HTTPS traffic are typically not decrypted? (Select two)

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

Answer: AB

4.Which Edge SWG component is responsible for analyzing and classifying web threats before allowing access?

- A. Threat Intelligence Engine
- B. Authentication Proxy
- C. SSL Certificate Verifier
- D. SSL Certificate Verifier

Answer: A

5.How can administrators offload HTTPS traffic to an SSL Visibility Appliance to enhance performance?

- A. By forwarding decrypted traffic from Edge SWG to the SSL Visibility Appliance
- B. By disabling SSL interception in Edge SWG
- C. By configuring Edge SWG to route all HTTPS traffic directly to the internet
- D. By using DNS filtering instead of SSL decryption

Answer: A