Boost up Your Certification Score

Broadcom

250-588

Broadcom Symantec Web Protection - Cloud SWG R2 Technical Specialist



For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/250-588

Latest Version: 6.2

Question: 1

Captive Portal is enabled for an Explicit Proxy location, yet users' browsers never complete the credential challenge.
Which documented Captive Portal requirement should the administrator verify?
Response:

A. That browsers send the BC_AUTH_USER header
B. That browsers accept third-party cookies
C. That the location uses IKEv2 with a dynamic FQDN
D. That SEP clients run WCAP in tunnel mode

Answer: B

Explanation:
Captive Portal requires browsers to accept third-party cookies; it also needs the Cloud SWG root certificate in browsers and the Auth Connector. A browser blocking those cookies cannot complete the challenge.

Question: 2

An administrator adds a Content Filtering rule whose condition is the file type of the downloaded content.
Where does the policy editor place this rule, and when is it evaluated?
Response:

A. In Group A, evaluated first so the request never reaches the server
B. In the Policy Bypasses layer, ahead of TLS/SSL interception
C. In the Threat Protection layer, after all Content Filtering rules
D. In Group B, which is checked only when no Group A rule in the layer acts

Answer: D

Explanation:
A file-type condition can only be judged once the destination has returned content, so the editor places the rule in Group B. Group B rules are checked only when no Group A rule in the layer has triggered an action.

Question: 3

An office sends web traffic to Cloud SWG through an IPsec tunnel. The administrator wants policy rules and reports to reference Active Directory users and groups.
Which component supplies that user and group information to Cloud SWG?
Response:

A. Captive Portal
B. Cloud Traffic Controller
C. PAC File Management System
D. Auth Connector

Answer: D

Explanation:
The Auth Connector runs on an AD member server or domain controller and forwards user and group metadata to Cloud SWG; with IPsec it also maps IP addresses to users.

Question: 4

A company wants to stop sensitive files from being uploaded to cloud storage apps, and to give its CASB visibility into the cloud apps employees use.
Which two Cloud SWG integrations apply?
(Select two.)
Response:

A. Symantec DLP Cloud, inspecting uploads
B. CloudSOC integration
C. Hosted Reporting, forwarding Edge SWG access logs
D. Universal Policy Enforcement

Answer: A,B

Explanation:
DLP Cloud scans uploads, both files and typed content. Cloud SWG sends them over a secure ICAP link to the DLP Cloud Detection Service and allows or blocks according to its verdict.
In the CloudSOC Audit solution Cloud SWG delivers its access logs to CloudSOC; the Gateway and CASB Only solutions extend that to enforcement and traffic steering.

Question: 5

An organization's laptops already run SEP clients managed from SEPM. It will use Web and Cloud Access Protection in tunnel mode to send their web traffic to Cloud SWG.
Which two statements about this deployment are true?
(Select two.)
Response:

A. The WSS Agent must also be installed on each laptop alongside SEP
B. An integration token from the portal is entered in SEPM
C. Users can switch the protection off themselves under the default policy
D. Seamless Identification removes the need for captive portal

Answer: B,D

Explanation:
Tunnel mode uses an integration token generated in the Cloud SWG portal and entered in SEPM or SES, linking the SEP clients to the tenant.
In tunnel mode, Seamless Identification passes the logged-in user to Cloud SWG, so captive portal is not required. Group-based policy still depends on the Auth Connector.

Question: 6

Employees work from home and while traveling, outside any defined Cloud SWG location.
Which two Cloud SWG access methods are designed for these remote workers?
(Select two.)
Response:

A. WSS Agent
B. Web and Cloud Access Protection
C. Firewall/VPN (IPsec) from a branch firewall
D. Proxy Forwarding from an Edge SWG appliance

Answer: A,B

Explanation:
The WSS Agent redirects a roaming device's traffic to Cloud SWG, taking its configuration from the Cloud Traffic Controller and tunneling to the nearest data center when it is off a corporate location.
WCAP extends existing SEP or SES clients so that they send web traffic to Cloud SWG, which is why it is one of the two remote-worker methods in the course.

Question: 7

An administrator is investigating unusual web activity from one employee.
Which two capabilities does the Cloud SWG Report Center provide for this?
(Select two.)
Response:

A. A Forensic Report on one user, client IP, category or site
B. Streaming of access events to a cloud storage bucket
C. Drill-down from a report into Full Log Details
D. A record of admin sign-ins, sign-outs and policy edits

Answer: A,C

Explanation:
Report Center's Forensic Report focuses on a single user, client IP address, category or site, which suits an investigation into one employee.
Report Center reports support filters and drill-down to Full Log Details, so the administrator can move from a summary to the individual transactions.

Question: 8

Users can browse through Cloud SWG, but rules written for their AD groups never match.
What should the administrator verify first?
Response:

A. That the Report User role can reach Report Center
B. That users are identified and authenticated
C. That PII suppression is not hiding user names in the logs
D. That the response page shows an Error ID

Answer: B

Explanation:
Identity is what user and group rules match on. Traffic can reach Cloud SWG without it, so browsing works while group rules never fire; identification and authentication come first.

Question: 9

An administrator creates a Content Filtering rule that should apply only to members of the Marketing Active Directory group at an IPsec location.
What must be in place for Cloud SWG to match users against that group?
Response:

A. Placement of the rule in Group A so it is evaluated first
B. The Reviewer role assigned to each Marketing group member
C. XFF anonymization turned off so Cloud SWG can read user names
D. Group membership from an identity method such as the Auth Connector

Answer: D

Explanation:
A group-based rule can match only when Cloud SWG knows who the user is and which groups the user belongs to. At an IPsec location the Auth Connector supplies that directory data.

Question: 10

Every company laptop already runs a Symantec Endpoint Protection (SEP) client managed from SEPM. The company wants roaming users' web traffic sent to Cloud SWG without deploying a separate agent. Which access method should the administrator use?
Response:

A. The WSS Agent, installed alongside the SEP client
B. Explicit Proxy with a head office PAC file
C. Web and Cloud Access Protection (WCAP) in tunnel mode
D. Firewall/VPN (IPsec) from the head office firewall

Answer: C

Explanation:
WCAP extends existing SEP or SES clients to Cloud SWG, with settings users cannot tamper with. Tunnel mode is the recommended mode; the PAC-file mode is being deprecated.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

