PassQueen
a.k.a dumpsqueen.com

# Administration of Symantec ProxySG 6.7

## Symantec 250-556

**Version Demo**

**Total Demo Questions: 9**

**Total Premium Questions: 91**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

## QUESTION NO: 1

Which two (2) environments will IP surrogate credentials NOT work in? (Choose two.)

**A.** With devices that use Network Address Translation

**B.** Out-of-path deployments

**C.** Transparent deployments

**D.** Explicit deployments

**E.** Multi-user environments such as Citrix

## ANSWER: A E

**Explanation:**

IP surrogate credentials associate an authenticated user with the client source IP address observed by ProxySG. This method therefore depends on a reliable one-to-one relationship between a user and an IP address for the lifetime of the surrogate credential. With devices that use Network Address Translation, multiple users can be represented to the proxy by one translated source address. ProxySG cannot safely distinguish which individual user should own the IP-based surrogate, so credentials cannot be accurately associated with a specific user.

Multi-user environments such as Citrix have the same fundamental identity problem. Many separate user sessions can originate from a shared Citrix host IP address. An IP surrogate would represent the shared host rather than the individual session user, preventing dependable per-user authentication and policy enforcement. In these environments, a user-specific surrogate method, such as cookie or other supported credential mechanisms appropriate to the deployment, is required to preserve individual user identity. Broadcom's ProxySG documentation provides the authentication and surrogate-credential configuration context at ProxySG documentation; additional product knowledge resources are available through the Broadcom Knowledge Base.

## QUESTION NO: 2

Which two (2) functions can SNMP provide when configured on a ProxySG? (Choose two.)

**A.** Poll appliance statistics

**B.** Send event notifications as traps

**C.** Install Visual Policy Manager policy

**D.** Perform SSL interception

**E.** Update the WebFilter database

## ANSWER: A B

**Explanation:**

SNMP can be used by a management station to poll ProxySG operational statistics and to receive configured SNMP trap notifications. Polling enables external monitoring systems to collect values such as interface, system, and service statistics. Traps provide asynchronous notifications when configured events occur, allowing a monitoring system to react without waiting for its next polling interval.

SNMP should be configured with appropriate access restrictions and secure community or user settings. ProxySG administration guidance is available from the Broadcom ProxySG documentation portal.

## QUESTION NO: 3

How do policy checkpoints evaluate the installed policy on a ProxySG? (Choose the best answer.)

**A.** At each checkpoint, a decision is made whether to allow or deny the transaction

**B.** The Server In checkpoint decides which rules will be evaluated by the other checkpoints

**C.** Relevant rules are evaluated at each checkpoint based on the information about the transaction that is available at that point

**D.** The Client In checkpoint decides which rules will be evaluated by the other checkpoints

## ANSWER: C

**Explanation:**

Relevant rules are evaluated at each checkpoint based on the information about the transaction that is available at that point. ProxySG policy processing is staged through transaction checkpoints, and each checkpoint has access only to the attributes that ProxySG has learned or established by that stage of handling the connection or request. For example, early processing can use client-side connection details, while later stages can use destination-server, request, response, and content information that becomes available only after the transaction progresses. The appliance evaluates policy rules that are relevant to the active checkpoint and applies the actions specified by the matching rule. This checkpoint-based evaluation lets administrators write policy that uses the appropriate transaction properties without requiring all information to be available at the start of a connection. Policy evaluation therefore is not simply a single universal allow-or-deny decision repeated identically at every stage; it is contextual evaluation of installed rules as additional transaction information is available. This model is fundamental to writing effective Visual Policy Manager and Content Policy Language rules for ProxySG. Symantec/Broadcom documentation for ProxySG policy and CPL provides the checkpoint model and the transaction-layer context in which policy rules are evaluated; see the ProxySG 6.7 documentation portal and the Broadcom Knowledge Base.

## QUESTION NO: 4

What does an action specify in Content Policy Language (CPL)? (Choose the best answer.)

**A.** The behavior applied when policy conditions match

**B.** The order in which policy layers are installed

**C.** The source address of a client connection

**D.** The syntax used to define a condition

## ANSWER: A

**Explanation:**

An action specifies the **behavior applied when the policy conditions match**. CPL conditions test properties of a transaction, such as the client, URL, protocol, or authenticated user. When the relevant conditions evaluate as true, the associated action determines what ProxySG does, such as allowing or denying access, requiring authentication, modifying headers, or applying a forwarding decision.

ProxySG policy documentation, including Content Policy Language information, is available through the ProxySG documentation portal.

## QUESTION NO: 5

How does a network administrator access sysinfo files? (Choose the best answer.)

**A.** Through the CLI

**B.** Through the Management Console

**C.** By creating a sysinfo layer in the VPM

**D.** Through the use of an advanced URL in a browser

**ANSWER: D**

**Explanation:**

Through the use of an advanced URL in a browser is correct. ProxySG provides its Sysinfo diagnostic output through a special, appliance-hosted URL rather than as a normal Management Console page or a Visual Policy Manager object. An administrator connects to the ProxySG appliance with a web browser and uses the appropriate advanced Sysinfo URL, authenticating with administrative credentials when prompted. The resulting Sysinfo output collects detailed appliance configuration, version, status, logging, and diagnostic information that is useful for troubleshooting and for providing information to support. Because Sysinfo can include sensitive configuration and operational details, access should be limited to trusted administrators and handled according to the organization's support-data procedures. This browser-based mechanism also makes the information easy to view or save for later analysis without requiring a policy change. ProxySG administration and diagnostic functionality is documented in Broadcom's ProxySG documentation library: Broadcom ProxySG documentation. Broadcom's support knowledge base is also the authoritative source for appliance-specific diagnostic collection guidance: Broadcom Knowledge Base.

## QUESTION NO: 6

Where does ProxySG object caching usually result in the most bandwidth savings? (Choose the best answer.)

**A.** On the server side

**B.** On the ProxySG

**C.** On the client side

**D.** On the enterprise WAN

**ANSWER: A**

**Explanation:**

**On the server side** is correct. ProxySG caching stores cacheable responses after retrieving them from an origin server. When subsequent client requests match a fresh cached object, the ProxySG can satisfy those requests locally rather than requesting the same object again from the origin server. Consequently, the repeated response traffic is avoided on the network path between the ProxySG and the origin/content server—commonly the upstream Internet or WAN connection. This is the server-side bandwidth that caching most directly conserves.

The amount saved is especially significant when many users request the same relatively static, cacheable resources, such as software downloads, images, style sheets, scripts, and other public web objects. One upstream retrieval can populate the cache, after which many downstream requests can be served without consuming additional origin-side bandwidth for that object. HTTP caching behavior, including freshness and reuse of stored responses, is defined in RFC 9111: HTTP Caching. Broadcom's ProxySG documentation is available through the ProxySG documentation portal.

## QUESTION NO: 7

Which two (2) characteristics make cookie surrogate credentials useful in a shared-IP-address environment? (Choose two.)

**A.** They can distinguish users who share a source IP address

**B.** They require the browser to return a surrogate cookie

**C.** They depend on a unique client IP address for each user

**D.** They eliminate the need for an authentication realm

**E.** They require the client to use a static IP address

**ANSWER: A B**

**Explanation:**

Cookie surrogate credentials associate an authenticated identity with a browser cookie rather than only with the client IP address. This allows ProxySG to distinguish browser sessions used by different users who appear to originate from the same source address, such as users behind NAT or on a shared terminal server. Cookie surrogates also require the browser to accept and return the configured surrogate cookie so ProxySG can recognize the authenticated session on later requests.

Authentication and surrogate credential configuration are documented in the ProxySG 6.7 documentation.

## QUESTION NO: 8

What is the purpose of a layer guard in Visual Policy Manager? (Choose the best answer.)

**A.** It determines whether the policy layer is evaluated.

**B.** It specifies the default action for unmatched rules.

**C.** It identifies the log facility used by the layer.

**D.** It determines the order in which all policy layers are installed.

**ANSWER: A**

**Explanation:**

A layer guard defines the condition under which a policy layer is evaluated. Before ProxySG processes the rules contained in a guarded layer, it evaluates the guard condition. If the transaction does not meet that condition, ProxySG skips the layer and continues processing the applicable policy. Layer guards are useful for limiting an entire layer to a particular client population, protocol, destination, or other transaction context without adding the same condition to every rule in the layer.

For ProxySG policy and Visual Policy Manager administration information, see the ProxySG 6.7 documentation.

## QUESTION NO: 9

Which two (2) ProxySG functions depend on accurate system time? (Choose two.)

**A.** SSL/TLS certificate validation

**B.** Access and event log timestamps

**C.** WebPulse URL categorization

**D.** Proxy-service listener selection

**E.** Apparent data type detection

**ANSWER: A B**

**Explanation:**

Accurate system time is important for **SSL/TLS certificate validation** and for **accurate log timestamps**. Certificate validation checks whether a certificate is within its valid date range, so an incorrect appliance clock can cause valid certificates to appear expired or not yet valid. Accurate timestamps are also necessary for correlating ProxySG access and event logs with records from authentication servers, SIEM systems, and other network devices.

Administrators commonly configure Network Time Protocol (NTP) to maintain appliance time. ProxySG configuration guidance is available in the ProxySG 6.7 documentation.