Blue Coat Proxy Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Is it true that the Blue Coat Management Center cannot be used to configure a ProxySG until an IP address has been assigned to it?**

   A. True

   B. False

   C. Only in explicit mode

   D. Only in transparent mode

2. **True or false: Access logging is disabled by default, requiring configuration to log intercepted protocols on the ProxySG.**

   A. True

   B. False

   C. Only for specific protocols

   D. Only for external connections

3. **What is the purpose of the VPM-XML file?**

   A. It stores the visual state of the VPM user interface

   B. It generates the CPL for the VPM

   C. It modifies the rules dynamically

   D. It stores user credentials for access control

4. **In the VPM, access logging is controlled by which type of objects?**

   A. Action objects

   B. Condition objects

   C. Protocol objects

   D. Rule objects

5. **What would happen if the ProxySG did not use surrogate credentials to authenticate users who use transparent proxy connections?**

   A. Users would be banned from accessing certain domains

   B. They would have to reauthenticate for each domain they access

   C. Traffic would be encrypted by default

   D. Access would be completely blocked

6. In an HTTP transaction, what does the response header contain?

A. Client information

B. Server configuration details

C. Status and metadata about the response

D. Only the data body

7. Which categories of traffic are typically not decrypted?

A. Educational services and Marketing

B. Financial services and Health

C. Entertainment and Social media

D. Government and Public sector

8. What is the outcome when a user connects to the ProxySG and authorization fails?

A. The user receives a success message

B. The user is redirected to the login page

C. The user gets access after retrying

D. The user receives a failure response code

9. Why is Kerberos performance generally considered superior to NTLM?

A. It requires less authentication

B. It uses less encryption

C. Only two round trips are needed between the browser and an authentication server

D. None of these answers

10. What are the two types of ProxySG exceptions?

A. Default and Custom

B. Pre-defined and User-defined

C. Automatic and Manual

D. Standard and Extended

Answers

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

Explanations

1. Is it true that the Blue Coat Management Center cannot be used to configure a ProxySG until an IP address has been assigned to it?

A. True

B. False

C. Only in explicit mode

D. Only in transparent mode

The statement is true because the Blue Coat Management Center requires communication with the ProxySG to perform any configuration tasks. Without an assigned IP address, the ProxySG cannot be properly integrated into the network, leading to communication issues between the management center and the proxy device. This IP address serves as the network identifier allowing the Management Center to recognize and connect to the ProxySG. Therefore, configuration cannot proceed until the device is network-ready with an IP address, making the answer correct. Assigning an IP address is a fundamental step in network configuration, ensuring that devices can interact and be managed effectively. Hence, the dependency on the IP address is crucial before establishing any connections that would facilitate configuration through the Management Center.

2. True or false: Access logging is disabled by default, requiring configuration to log intercepted protocols on the ProxySG.

A. True

B. False

C. Only for specific protocols

D. Only for external connections

Access logging being disabled by default on the ProxySG is accurate and reflects a common practice in security and network appliances. When access logging is turned off by default, it is a measure taken to enhance privacy and reduce performance overhead without configured logging. Network administrators must explicitly enable access logging to monitor and log intercepted protocols that the ProxySG is handling. This default state underscores the need for proper configuration based on organizational needs before deploying the proxy in a live environment. In contrast, other choices focus on conditions that do not align with the general behavior of the ProxySG's logging mechanisms, such as suggesting that logging might be enabled for certain protocols or only for external connections. The default setting applies universally across the entire proxy operation until logs are specifically configured to capture necessary data.

3. What is the purpose of the VPM-XML file?

A. It stores the visual state of the VPM user interface

B. It generates the CPL for the VPM

C. It modifies the rules dynamically

D. It stores user credentials for access control

The VPM-XML file serves a specific purpose related to the visual representation of the VPM (Visual Policy Manager) user interface. By storing the visual state, it helps maintain a consistent and user-friendly experience for users interacting with the policy management tool. This includes saving information such as the layout, organization of elements, and any user-defined settings that contribute to how the interface appears and functions at any given time. The other choices do not accurately reflect the primary function of the VPM-XML file. While it may seem intuitive to associate dynamic modifications or access control capabilities with XML files due to their structured nature, these functions are handled through other mechanisms within the VPM architecture. Understanding the visual state aspect emphasizes the importance of user experience in managing policies effectively using the VPM interface.

4. In the VPM, access logging is controlled by which type of objects?

A. Action objects

B. Condition objects

C. Protocol objects

D. Rule objects

Access logging in a VPM (Visual Policy Manager) is primarily managed by action objects. These objects define the specific actions taken when a request matches a rule in the VPM policy. When it comes to logging access, action objects determine what kind of logging will occur after a condition has been met. This includes specifying whether to log allowed or denied requests, setting the logging level, and more. The focus of action objects on defining the behavior that takes place as a result of evaluating conditions makes them essential for managing how access logs are generated. They are designed to reflect the desired outcome of applying policy rules, which includes capturing relevant data regarding user activity for security and compliance monitoring. In contrast, condition objects serve to establish the criteria that must be satisfied for the associated actions to trigger, protocol objects define the specific protocols to which actions and conditions apply, and rule objects are the overall structures that bring together conditions and actions. Therefore, while all play vital roles in VPM policies, it is the action objects that specifically control the logging aspect of access management.

5. What would happen if the ProxySG did not use surrogate credentials to authenticate users who use transparent proxy connections?

A. Users would be banned from accessing certain domains

B. They would have to reauthenticate for each domain they access

C. Traffic would be encrypted by default

D. Access would be completely blocked

Using surrogate credentials in a Blue Coat ProxySG when handling transparent proxy connections allows for a seamless authentication experience for users. If surrogate credentials are not implemented, users would be required to reauthenticate each time they access a new domain. This is because the ProxySG would not have a pre-existing authenticated session for the user across different domains, necessitating a fresh authentication process for each distinct request. This requirement can create significant friction for users as it interrupts their browsing experience and can lead to frustration, particularly in environments where users access a variety of sites frequently. By using surrogate credentials, the ProxySG maintains the authentication context, allowing users to engage with multiple domains without repeated logins. This also enhances overall efficiency and user satisfaction in network access scenarios.

6. In an HTTP transaction, what does the response header contain?

A. Client information

B. Server configuration details

C. Status and metadata about the response

D. Only the data body

In an HTTP transaction, the response header plays a crucial role as it contains status information and metadata about the response sent from the server to the client. This header includes important pieces of information such as the HTTP status code (which indicates whether the request was successful or if there was an error), content type, content length, caching directives, and other context that helps the client understand how to handle the response. For example, the status code like 200 OK signifies a successful request, while other codes like 404 Not Found or 500 Internal Server Error provide error information. Additionally, metadata such as the date the response was generated, server type, and any session or cookie-related data are included in the response header, aiding in proper communication and interpretation of the data that follows in the body of the response. In contrast, client information alone does not provide a comprehensive view of the transaction state, server configuration details are not part of the response header (rather they might be included in specific headers), and the response cannot be accurately described as containing only the data body, as that would neglect the essential metadata and status information provided in the response header.

7. Which categories of traffic are typically not decrypted?

A. Educational services and Marketing

B. Financial services and Health

C. Entertainment and Social media

D. Government and Public sector

Traffic related to financial services and health is typically not decrypted due to stringent regulations and privacy concerns. Financial services involve sensitive information such as banking details, credit card numbers, and transaction records, which are protected under various laws like the Gramm-Leach-Bliley Act and PCI DSS (Payment Card Industry Data Security Standard). Similarly, health-related information is safeguarded by regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States, which mandates the protection of personal health information. Decryption of this data could expose individuals to identity theft and fraud, as well as violate legal protections designed to keep such information confidential. Therefore, organizations handling this type of traffic generally opt to implement strong encryption protocols to maintain compliance and protect user privacy, leading to limited or no decryption of these data categories. Other options may involve less regulatory scrutiny, thus allowing for more flexibility in traffic management practices, potentially making them more amenable to decryption. However, the critical nature of security and privacy in financial and health services ensures they remain protected from decryption efforts.

8. What is the outcome when a user connects to the ProxySG and authorization fails?

A. The user receives a success message

B. The user is redirected to the login page

C. The user gets access after retrying

D. The user receives a failure response code

When a user connects to the ProxySG and authorization fails, they receive a failure response code. This response code indicates that the authorization process was unsuccessful and therefore the user is not permitted access to the requested resource. The ProxySG is designed to enforce security policies, and when a user does not meet the criteria required for authorization, it provides a clear signal through a failure response code. This approach helps to maintain security and integrity by ensuring that only authorized users can access certain resources. In a proper authorization workflow, a failure response code serves as a mechanism to inform the user or system initiating the connection that their credentials are invalid or that they do not have the necessary permissions to proceed. In contrast, the other outcomes listed—such as receiving a success message, being redirected to a login page, or gaining access after retrying—do not align with the expected behavior of a secure proxy system when authorization is denied. In such systems, a failure response code is critical to delineate between authorized and non-authorized access attempts.

9. Why is Kerberos performance generally considered superior to NTLM?

A. It requires less authentication

B. It uses less encryption

C. Only two round trips are needed between the browser and an authentication server

D. None of these answers

Kerberos performance is generally regarded as superior to NTLM largely due to its efficient use of network resources, which is highlighted by the requirement of only two round trips between the browser and the authentication server for obtaining a ticket-granting ticket (TGT) and a service ticket. This streamlined process significantly reduces latency and enhances overall performance compared to NTLM, which can be more cumbersome and resource-intensive due to its reliance on multiple authentication requests and challenges, requiring more interactions between client and server. In contrast, the other options do not accurately capture the essence of Kerberos's performance benefits. While it's true that Kerberos is designed to provide robust security features, its advanced structure that minimizes the number of required communications is a key factor that contributes to its superior performance compared to NTLM. This unique two-round trip mechanism in Kerberos makes it more efficient for environments where quick authentication is critical.

10. What are the two types of ProxySG exceptions?

A. Default and Custom

B. Pre-defined and User-defined

C. Automatic and Manual

D. Standard and Extended

The two types of ProxySG exceptions, identified as pre-defined and user-defined, reflect the flexibility and functionality available within ProxySG configurations. Pre-defined exceptions are those that come built-in with the system; these are standard exceptions that address common scenarios and are ready for implementation without requiring additional setup. Examples might include common web access patterns or typical security exceptions. On the other hand, user-defined exceptions allow administrators to create customized exceptions tailored to their specific environment or needs. This is particularly important in organizations where standard exceptions may not adequately cover unique web traffic patterns or security protocols required for special applications or workflows. By providing both pre-defined and user-defined options, ProxySG allows for greater adaptability and specificity in managing web traffic and security protocols, ensuring that organizations can customize their configurations to fit their operational requirements effectively.