



Executive Summary

As the leader in Wide Area Application Delivery, Blue Coat products accelerate and secure applications within your WAN and across the Internet. Blue Coat provides a robust and flexible solution that controls users and network resources, protects against Web-based threats, and accelerates the broadest range of WAN-based applications. Whether deployed on either end of a WAN, at Internet access points, or in front of business-critical services, Blue Coat ProxySG appliances provide control points that stop the bad and accelerate the good. As part of this solution, flexible access control through authentication and authorization is a requirement. Guest Authentication provides a key component to this flexibility, providing administrators with the ability to selectively allow non-authenticated users access to network resources.

What is Guest Authentication?

Guest Authentication is an authentication feature that enables administrators to permit users to access the network as guests, assigning them various authentication and authorization attributes. Using Guest Authentication, users who would have been considered unauthenticated and/or denied can be allowed to successfully make network requests. Guest Authentication is often implemented in conjunction with Blue Coat's Permit Authentication Error feature, which allows users to access network resources when specific authentication failures occur.

Why should I implement Guest Authentication?

Most security-conscious enterprises today implement some form of authentication and authorization for accessing network resources. The benefits to this approach are clear — user permissions can be verified before granting network access to resources, and user activity can be monitored through various logging mechanisms. There are, however, some enterprises that find authentication and authorization desirable, but not necessarily required for users to access resources. Some administrators would like to avoid authentication for certain users altogether and simply track the user as an unauthenticated guest, while others prefer that authentication and authorization is attempted but that user requests are allowed and tracked as guests if certain authentication and authorization errors are encountered (Permit Authentication Error used in conjunction with Guest Authentication). There are numerous reasons why authentication and authorization can fail, including invalid credentials and failure to connect to the external authentication server. Some administrators would like the flexibility to allow user transactions to continue in the event of an external authentication server failure, but terminate user transactions that explicitly offer invalid credentials. Others may want to extend a subset of network services to non-authenticated users, such as providing Internet-only access to non-employee wireless users onsite. Guest Authentication makes these types of flexible authentication policies possible.

How does Guest Authentication work?

Guest Authentication works by identifying users as guest users and allowing them to make requests without requiring that they successfully authenticate. Identification of a guest user can occur in several ways. Users can be automatically identified as guests without any authentication and authorization challenge. Alternately, users who encounter specific authentication and authorization errors can be identified as guests. Guest users can also be identified during the authentication and authorization challenge process by presenting them with a guest user option. In all scenarios the user is identified as a guest user, assigned



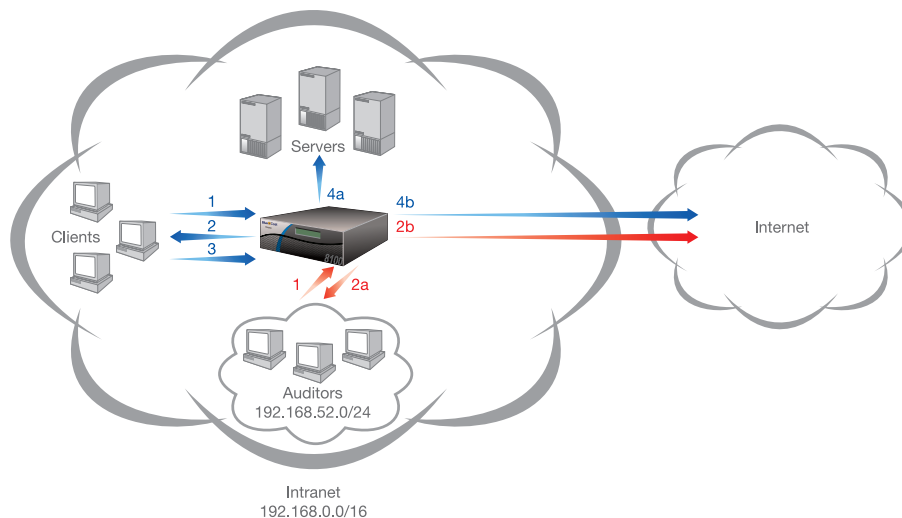
a guest username, and recognized as authenticated for the specified realm. Guest users can also be assigned to default groups within the realm so that group-based policy can be implemented. Because users are assigned a guest username and realm, guest access can be identified in the ProxySG access logs and are subject to guest-specific policies, if defined.

Typical Use Cases

- > Identify users as guests who are not logged into the single sign-on domain.
- > Identify users as guests if an authentication server failure occurs.
- > Automatically identify users as guests based on client IP address or destination request.

Example 1a

A network administrator has successfully implemented forms-based LDAP authentication on the local ProxySG appliance. All users must be authenticated and authorized before requests are allowed (the default is to deny all requests). There is a group of auditors who will be onsite for one week and will require Internet access. They will all be placed on a unique subnet so that they can be identified on the network. The administrator will grant them guest user access for external (Internet-bound) requests only. The behavior for user requests are as follows:



Network user accessing network resource or Internet content

- 1 User requests network resource or Internet content.
- 2 User is challenged for authentication credentials.
- 3 User provides credentials.
 - 3a User is authenticated based on credentials and authorization information is obtained.
- 4a User access to network resource is granted.
- 4b User access to Internet content is granted.

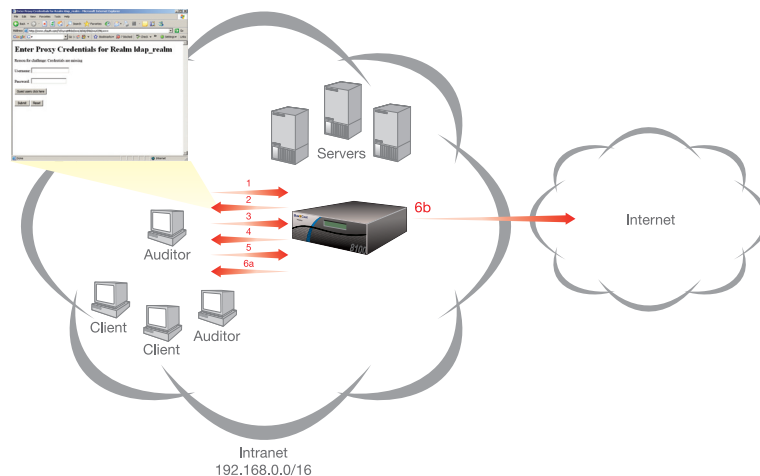
Auditor accessing network resource or Internet content

- 1 Auditor requests network resource or Internet content.
 - 1a Auditor is identified as a "guest user" based on source IP.
 - 1b Auditor's request is identified as a network resource or Internet content.
- 2a Auditor access to network resource is denied.
- 2b Auditor access to Internet content is granted.



Example 1b

The administrator in the first example has discovered that the auditors will not be accessing the network from the same subnet as initially believed. Instead, the auditors will be accessing the network from various locations and will not have static IP addresses. The administrator therefore decides to modify the existing authentication form to include a guest user link, which when selected will result in guest user identification of the user. This results in the following alternate behavior for auditor requests.



Auditor accessing network resource or Internet content

- 1 Auditor requests network resource or Internet content.
- 2 Auditor is challenged for authentication credentials.
 - 2a Auditor clicks on "Guest users click here" on the authentication form presented.
- 3 Auditor requests guest user link.
 - 3a Blue Coat policy identifies the auditor as a "guest user" based on the guest user link.
- 4 Blue Coat ProxySG returns a redirect to the original request.
- 5 Auditor is automatically redirected to the original request by the browser.
 - 5a Auditor's request is identified as a network resource or Internet content.
- 6a Auditor access to network resource is denied.
- 6b Auditor access to Internet content is granted.

Blue Coat Difference

Flexible User Authentication

Many of the authentication and authorization solutions available today support either authenticating users or allowing them to bypass authentication altogether. This results in a loss of visibility, some loss of control, and even loss in functionality for the user who may require specific group membership to successfully conduct business. As any administrator knows, network access is not always so black and white. The ability to handle the shades of grey with which administrators are sometimes presented can therefore be key in ensuring that network activities continue "business as usual".

Visibility

Guest Authentication ensures that a major requirement for network administrators – visibility – is met. By assigning unauthenticated users usernames (and optionally groups), unauthenticated user requests can be monitored via access logs and reported on just like authenticated users.

User-Based Policy

The ability to identify users as guests not only provides visibility into user behavior, but also enables administrators to control guests with user-based policies. By creating user-based policies, administrators can not only dictate how, when, and where guest users make requests, but also apply other policy features to guest users such as imposing bandwidth management restrictions.