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, ProxySG appliances support Authentication, Authorization, and Accounting, which provide user-level control of connections.

What is Authentication, Authorization, and Accounting?
Authentication, Authorization, and Accounting (AAA) is the process of identifying a user, determining the permissions granted to that user, and keeping a record of that user’s activity. Using AAA, you can identify users, determine their group memberships and attributes, and use that information to implement access control policies to effectively control what people are allowed to do on the network (while keeping a record of all transactions).

Why should I perform Authentication, Authorization, and Accounting?
One of the basic functions of a ProxySG appliance is to provide control over network connections. As part of the solution, it is often desirable to exercise that control on a user or group basis; for example, limiting access to resources that should be available only to the Executive team, restricting internet access to only certain groups, or implementing bandwidth control based on user or group membership. These objectives can be achieved with AAA. Most enterprises use some form of AAA in the network, often to control access to network resources. When a ProxySG appliance is deployed, administrators can choose to have the ProxySG appliance use the existing authentication architecture to identify users and determine their group memberships and attributes. (In deployments that do not have an existing authentication mechanism, a Local password file can be used to define users and groups). After authentication is configured, administrators can create user and group-based policy to manage and monitor access to content, both internal and external. The ability to employ user, group, or attribute information in the decision making process allows administrators to have more granular control over connections and content. AAA also enables the ProxySG appliance to associate users with client requests and log those requests in an access log. This Accounting component of AAA is sometimes required by enterprises to comply with local or international laws.

How does Authentication, Authorization, and Accounting work?
As the name suggests, there are three distinct components to AAA - Authentication, Authorization, and Accounting. Authentication is the process of verifying, or determining, the identity of a user and most often begins with the ProxySG appliance sending a credential challenge in response to the user’s initial request. The user responds to the challenge by sending credentials to the ProxySG appliance, which passes them to the authentication server for verification. If the credential verification succeeds, the user identity is known and group and attribute information for that user can also be obtained. The ProxySG appliance uses that information, as well as configured policy, to authorize, or make decisions on how to handle, the user’s requests. As part of the process, user requests are logged in the ProxySG appliance access log, thus providing the Accounting.
Authentication Realms

While most authentication schemes support the determination of user identity and group and attribute values, some schemes support only user identity. For some deployments, user identification is the only requirement; others couple one authentication scheme with another to achieve a full solution. Blue Coat ProxySG appliances use authentication realms to define which authentication schemes to use. The following authentication realms support determination of both user and group information:

- **IWA** – Integrated Windows Authentication using Kerberos, NTLM or Basic credentials.
- **LDAP** – Authentication against LDAP servers. Popular LDAP servers include Active Directory, Novell eDirectory and Netscape iPlanet.
- **RADIUS** – Authentication against RADIUS servers.
- **Local** – Authentication using a password file installed locally on the ProxySG appliance.
- **Oracle COREid** (also known as Oracle Access Manager and formerly Oblix COREid) – Authentication integration with Oracle COREid systems. Supports COREid single sign-on deployments.
- **Netegrity SiteMinder** (also known as CA eTrust SiteMinder) – Authentication integration with Netegrity SiteMinder systems. Supports SiteMinder single sign-on deployments.

For LDAP and RADIUS authentication, the ProxySG appliance contacts the authentication server directly. IWA, COREid and SiteMinder authentication use an intermediary agent, the Blue Coat Authentication and Authorization Agent (BCAAA), to integrate with the authentication server.

For some deployments, identifying users via a credential challenge is not desirable, or is not possible. Because of this, ProxySG appliances support authentication schemes that allow users to be identified by other methods; instead of the ProxySG appliance issuing a user challenge, the user is authenticated based on information in the client request. Since there is no contact with an authentication server as part of the identification process, group and attribute information is not obtained. That information can be determined, however, by configuring a separate authentication realm such as LDAP or Local. The following authentication realms use an authentication scheme that verifies users only:

- **Certificate** – Authenticates the user using a user certificate.
- **Policy Substitution** – Identifies the user using various information from the user’s request.
- **Windows SSO** – Identifies the user by mapping the client request IP address to a Windows domain login.

Authentication Modes

Blue Coat ProxySG appliances support a variety of authentication modes that specify the type of authentication challenge and surrogate credentials to use. The authentication challenge is the method of obtaining user credentials from the client. The
available challenge methods are:

- **Origin** – Challenges using a 401 Authenticate request. Commonly used in reverse proxy deployments.
- **Origin-redirect** – Redirects the user request to a virtual URL before issuing an origin challenge. Commonly used in transparent deployments.
- **Proxy** – Challenges using a 407 Proxy-Authenticate request. Commonly used in explicit proxy deployments.
- **Forms** – Challenges using an authentication form. Allows customization of the information displayed in the user challenge.
- **Form-redirect** – Redirects the user request to a virtual URL before issuing a form challenge.

To reduce the number of challenges issued to users and the amount of traffic generated between the ProxySG appliance and the backend authentication servers, the ProxySG appliance supports the use of surrogate credentials. Surrogate credentials are credentials accepted in place of a user’s actual credentials. The following surrogate credentials are supported:

- **Connection** – The user is only authenticated once per connection.
- **Cookie** – An authentication cookie is set after successful authentication and offered in subsequent requests.
- **IP address** – The user’s IP address is used to map to an authenticated user. IP surrogates are useful when implementing authentication schemes that rely on unique IP addresses (e.g. Windows SSO) or when user agents do not support cookies.

It is important to note that even when the authentication method specifies the use of cookie or IP surrogates, a user will only be authenticated once per connection.

The ProxySG appliance supports various combinations of the preceding challenge methods and surrogate credentials. There is also an “auto” mode that determines and uses the optimum authentication mode on a per-request basis.

**The Blue Coat Authentication and Authorization Agent (BCAAA)**

The Blue Coat Authentication and Authorization Agent (BCAAA) is a software agent that is installed and configured separately from SGOS. The BCAAA acts as an intermediary service between the ProxySG appliance and certain authentication schemes. For IWA, the BCAAA is installed on a domain member server and uses Windows APIs to authenticate the user and obtain group information. For Oracle COREid, access to the COREid Access System is routed through the BCAAA, with the BCAAA acting as a custom Access Gate within the COREid Access System. The BCAAA communicates with the COREid Access Servers to authenticate the user and to obtain a COREid session token, authorization actions, and group membership information. HTTP header variables and cookies specified as authorization actions are returned to BCAAA and forwarded to the ProxySG appliance. The BCAAA is also required for Netegrity SiteMinder authentication and is supported on both Windows and Solaris. Within the SiteMinder system, BCAAA acts as a custom Web agent, communicating with the SiteMinder policy server to authenticate the user and to obtain a SiteMinder session token, response attribute information, and group membership information. Custom header and cookie response attributes associated with OnAuthAccept and OnAccessAccept attributes are obtained from the policy server and forwarded to the ProxySG appliance.
The BCAA is also used as part of the Windows SSO scheme and can be configured to monitor domain controllers for user logins and/or query client machines for user login information.

**Sequence Realms**

Blue Coat ProxySG appliances support the use of sequence realms for authentication. Sequence realms are used to combine a variety of authentication realms. The ProxySG appliance will attempt to authenticate the user against each realm in the sequence until a successful authentication is achieved. Sequence realms are particularly useful for organizations that want to support multiple authentication realms, but are unable to easily map a user request to a particular realm. Sequence realms are also commonly used to specify the priority of authentication checking. For example, the sequence realms can specify that a primary authentication scheme such as IWA or LDAP be tried first, and if that fails to try an SSO scheme such as Windows SSO or policy substitution.

**Authorization via Policy**

Authorization of user requests is achieved through the implementation of Blue Coat Policy, allowing administrators to define powerful user or group-based policies to manage and monitor access to both internal and external content. ProxySG appliances support several authentication-specific policy conditions and properties for this purpose.

**Example Authentication and Authorization Policy**

An administrator at Blue Coat Systems wants to authenticate users only when they are accessing the Internet; intranet access does not require authentication. When accessing the Internet, access to certain types of Web sites will not be allowed for the general employee population, but will be made available to certain organizations within the company that may need access to those sites for business purposes. Executives will have no restrictions.

```xml
<PROXY>
  url.domain=intranet.bluecoat.com ALLOW
  authenticate(NTLMRealm)
</PROXY>
<PROXY>
  group=cf-cal\executives ALLOW
  group=cf-cal\hr category=("Travel", "Job Search/Careers") ALLOW
  category=("Travel", "Job Search/Careers", "Gambling","Nudity") exception [content_filter_denied]
</PROXY>

*the default policy is ALLOW*

**Accounting via Access Logging**

Blue Coat appliances can be configured to keep a record of all client requests in the form of an access log. Several predefined access log formats are available and custom formats can be created. For AAA purposes, the most important information that needs to be captured in the access log is the user and its associated request. Typical access log entries are as follows:

The following entry logs the username only using the "cs-username" access-log field.
2007-03-22 23:05:39 64 10.167.10.100 304 TCP_HIT 256 497 GET http www.google.ca 80 /images/nav_logo2.png - user1 - DIRECT 72.14.203.99 image/png http://www.google.ca/ ”Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)” PROXIED “none” - 10.167.42.28

The following entry logs the Fully Qualified Domain Name (FQDN) of the user using the “cs-userdn” access-log field.

2007-03-22 23:07:32 55 10.167.10.100 304 TCP_HIT 256 497 GET http www.google.ca 80 /images/nav_logo2.png - CN=user1,CN=Users,DC=authteam,DC=waterloo,DC=bluecoat,DC=com - DIRECT 72.14.203.99 image/png http://www.google.ca/ ”Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)” PROXIED “none” - 10.167.42.28

Blue Coat Difference

More Than Just Authentication and Authorization

The typical role of Authentication and Authorization is to identify users and use identity and authorization information to control access to network resources. With Blue Coat ProxySG appliances, Authentication and Authorization plays a much more powerful role. Information obtained through authentication and authorization can be used by administrators to make decisions regarding bandwidth, content filtering, internal/external content, virus scanning, and more based on user or group membership.

Breadth of Solution

Blue Coat provides a comprehensive Authentication, Authorization, and Accounting solution. The number of authentication schemes, challenge types, and surrogates supported allow ProxySG appliances to be deployed in almost any environment.