How to Integrate the Barracuda Web Security Gateway With a User Authentication Service

https://campus.barracuda.com/doc/6160400/

Granular Policies By Users, Groups or Machines

By integrating the Barracuda Web Security Gateway with your existing authentication server, you can configure usage policies at several levels of granularity; policies can apply to the whole organization or to specific users, machines, or groups. Using LDAP , NTLM , or Kerberos authentication, or a combination of them, you can apply policies and generate reports directly on users, LDAP organizational units (defined on your LDAP server) or groups you define without the need to create local user accounts on the Barracuda Web Security Gateway.

Note that neither NTLM or Kerberos are typically supported for multiple domains on one Barracuda Web Security Gateway; however, if this is required for your configuration, please contact Barracuda Networks Technical Support.

Integration with External Systems and Services - Security Considerations

The Barracuda Web Security Gateway integrates with other systems and services in your environment, like your LDAP, NTLM, or Kerberos servers. Barracuda recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy. For more information, see Security for Integrating with Other Systems - Best Practices.

Applying Web Access Policy by Groups

Typically, computer users in a network are grouped along organizational, departmental, physical or functional boundaries. As the administrator, you can create secure accounts for network users and also group them as appropriate. Users then supply their login credentials from their workstations to activate their network privileges. This allows the administrator to control Internet access privileges separately for each user or group of users. For example, a school can apply a more restrictive browsing policy for students than for teachers and staff, or an organization can allow access to job sites only to the Human Resources department (which you may have defined as an organizational unit on your LDAP server).

If you do not integrate with your LDAP, NTLM or Kerberos authentication server, you can apply filtering policy exceptions only to local users and groups that you create in the **USERS/GROUPS** tab.

Terminal Environments and Authentication

Kerberos and NTLM authentication schemes work well with Citrix terminal environments and Windows terminal services environments. The Barracuda Web Security Gateway can also support various user groups using different authentication schemes to provide different types of user access and policy control. For example, if your organization has a group of Windows desktop users who authenticate against an LDAP server and another group using a Citrix terminal environment or Windows terminal services environment, you can configure both groups with one Barracuda Web Security Gateway.

Using a 'hybrid' authentication deployment, Windows desktop users can authenticate inline via your LDAP server, while the terminal users can authenticate via NTLM or Kerberos in a forward proxy configuration.

To use a hybrid authentication scheme:

1. Add your LDAP and NTLM or Kerberos services as described in How to Choose Your Authentication Mechanisms and related articles.
2. Go to the **ADVANCED > Proxy** page.
3. Set **Enable Port Auth Exemption** to *Yes.* This means that port **8080** traffic is exempt from NTLM/Kerberos authentication.
4. Proxy Windows desktop traffic to port 8080 on the Barracuda Web Security Gateway.

Detailed procedural help is also available on the **ADVANCED > Proxy** page.

LDAP Authentication

LDAP users are authenticated when credentials are provided in order to proceed to a blocked or warned web page or application. LDAP users can also be authenticated by single sign-on access if you install the **Barracuda DC Agent** software on your domain controller(s) – see Barracuda DC Agent for User Authentication for details, or see the Help on the **USERS/GROUPS > Authentication** page. NTLM and Kerberos users are authenticated by single sign-on access against the NTLM or Kerberos authentication service, so they are transparently authenticated in the Barracuda Web Security Gateway using their Microsoft Windows credentials. Authenticated domain users are known by username, client IP address, and group membership:

- Usernames and client IP addresses of authenticated LDAP domain users are visible in the **USERS/GROUPS > Account View** page, the **Web Log** page, the **Application Log** page and

in reporting output.
- Group membership information about authenticated domain users is available by opening the **Lookup** facility (accessed by clicking **Lookup** button in the **BLOCK/ACCEPT > Exceptions** page) and using the **Active Directory User/Group** section of that window.

Note: Domain users that are *unauthenticated* in the Barracuda Web Security Gateway appear as *anonymous* users.