

The award-winning Barracuda Web Filter makes it easy for organizations to control access to Web sites and Web applications to protect networks from Web based threats, improve productivity and optimize usage of computing resources. Network administrators can configure usage policies at several levels of granularity; for the whole organization or for specific users, machines or groups. User or group level policy management is made very simple by integrating the Barracuda Web Filter with centralized network authentication systems. Through this, network administrators can apply policies and generate reports directly on users or groups as listed in central authentication servers without the need to create local user accounts on the Barracuda Web Filter.

Typically, computer users in a network are grouped along organizational, departmental, physical or functional boundaries. Authentication systems help administrators centrally manage user credentials and group relationships. Administrators can create secure accounts for their network users and also group them as appropriate. Users then supply these login credentials from their workstations to activate their network privileges. This allows administrators to control Internet access privileges separately for each user or groups 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 to the Human Resources department alone.

The Barracuda Web Filter can directly integrate with most popular authentication systems. By seamlessly integrating with commonly used authentication schemes including LDAP, NTLM and Kerberos, the Barracuda Web Filter facilitates plug-and-play deployment in most network environments. The various schemes supported by the Barracuda Web Filter include:

1. Directory Servers through LDAP

Directory servers are commonly used to provide user authentication and directory services in local area networks. The Barracuda Web Filter integrates with Directory servers using the Lightweight Directory Access Protocol (LDAP) which provides seamless access to all user and group information from the authentication server. This allows administrators to directly apply Web access policies to these users and groups, thereby simplifying policy management for large networks.

The configuration steps are as simple as specifying the hostname or IP Address, access port and access credentials of the LDAP server. Network users will be prompted to log in to the Barracuda Web Filter at the first browsing session by supplying their standard Windows login credentials. The Barracuda Web Filter will then authenticate the user against the LDAP server. Once user identity and group relationships are established, the user will be authenticated to the Barracuda Web Filter and will not have to log in again for a subsequent browsing session.

A single Barracuda Web Filter can integrate with multiple LDAP servers. Most popular Directory servers are supported, including OpenLDAP, Lotus Domino and Microsoft Active Directory.

2. Microsoft Active Directory through LDAP and DC Agent

While LDAP integration with directory servers requires users to authenticate to the Barracuda Web Filter as well as to their network domain, integration with Microsoft Active Directory servers can be further simplified by installing the Barracuda DC Agent Software on Windows Domain

Controllers. With the DC Agent, the Barracuda Web Filter can monitor the Windows Domain Controllers to automatically detect when users log in to their Windows Domains. This provides

true single sign-on capability by avoiding the need for users to log in to the Barracuda Web Filter at the first browsing session. Rather, the Barracuda Web Filter will recognize users when they log in to their Windows domains and seamlessly apply policies based on their Windows login credentials.

The Barracuda Web Filter also supports multiple domains, trusted domains and multiple domain controllers.

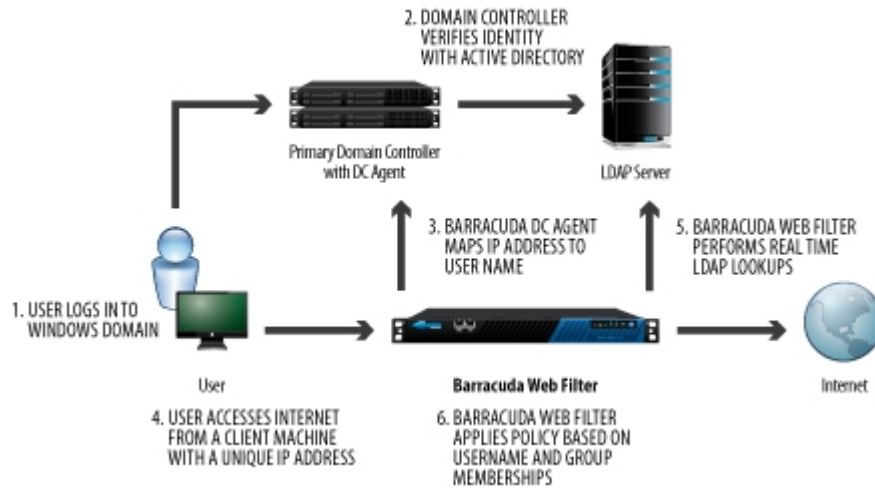


Figure 1. Active Directory through LDAP and DC Agent

3. Novell eDirectory through LDAP

Novell eDirectory is a popular authentication service used by enterprises and educational institutions. The Barracuda Web Filter can integrate with Novell eDirectory servers through LDAP to automatically detect user login events and gather user credentials. Administrators can apply Web usage policies to users and groups configured on the eDirectory server, and the Barracuda Web Filter will automatically identify the users as they log in to the domain and enforce the appropriate policy.

The Barracuda Web Filter can directly communicate with the Novell eDirectory server to perform fully transparent user authentication. Unlike Active Directory, this does not require DC Agents on the Domain Controller for single sign-on authentication.

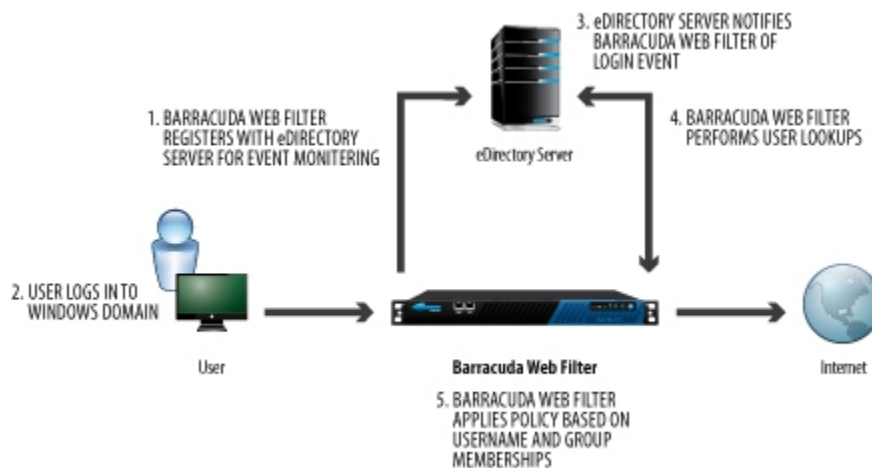


Figure 2. Novell eDirectory through LDAP

4. NTLM Authentication

NT LAN Manager (NTLM) is a challenge-response based protocol that is the default authentication mechanism for Windows NT platforms and is also available (in mixed-mode) in Windows 2000 and Windows 2003 Active Directory environments.

NTLM is a session-specific authentication scheme that does not rely on IP addresses to distinguish between users. This allows the Barracuda Web Filter to authenticate users even when they share IP addresses. Therefore, it is particularly useful for networks using CITRIX or Windows Terminal Services or when the clients are behind a NAT enabled router.

The Barracuda Web Filter can use NTLM to integrate with the authentication server when deployed as a forward proxy. By becoming a trusted host on the Windows Domain, the Barracuda Web Filter can access all user and group information from the Domain Controller so that administrators can directly specify Web usage policies on users and groups configured in their authentication server. Users are authenticated when they log in to their Windows Domains. Since the Barracuda Web Filter is a trusted host in the NTLM domain, it can extract the originating user credentials from each Web request and enforce appropriate policies.

As always, configuration is simple. The Barracuda Web Filter just needs to know the name of the NTLM domain, the IP address of the NTLM server and Domain controller information to join the Domain as a trusted host. There is no need for DC Agent software.

Integration through NTLM allows the Barracuda Web Filter to transparently identify authenticated NTLM domain users without requiring any additional agents or users logging in separately to the Barracuda Web Filter.

5. Kerberos Authentication

Windows 2000 (and later) platforms use Kerberos as the native authentication method. Kerberos provides mutual authentication; i.e. both the user and the server verify each other's identity.

Kerberos is considered a more secure authentication protocol than NTLM. Like NTLM it provides per-session authentication and policy control and it is a Forward proxy authentication scheme.

The Barracuda Web Filter can be easily integrated into environments using Kerberos authentication by becoming a trusted host in the Windows Domain. The Barracuda Web Filter can then gather user Windows Login credentials to detect user login events and apply user and group based policies through true single-sign-on transparent authentication.

Configuration involves generating a Key file from the active directory server and applying the appropriate account setting on the Barracuda Web Filter. The Barracuda Web Filter needs to know the host name of the domain controller, the valid user account to join to the Active Directory, and the Key file.

Kerberos support allows the Barracuda Web Filter to be integrated into networks using the native authentication scheme with Windows 2000 and later platforms.

By directly integrating with most popular Authentication schemes, the Barracuda Web Filter makes it simple for administrators to configure granular Internet access policies without the need for any additional user account management. This also enables the Barracuda Web Filter to be easily deployed in most existing network environments. Seamless user authentication combined with powerful malware protection, comprehensive content and application filtering and flexible policy management make the Barracuda Web Filter a fully integrated Network security solution that is easy to deploy, use and maintain.

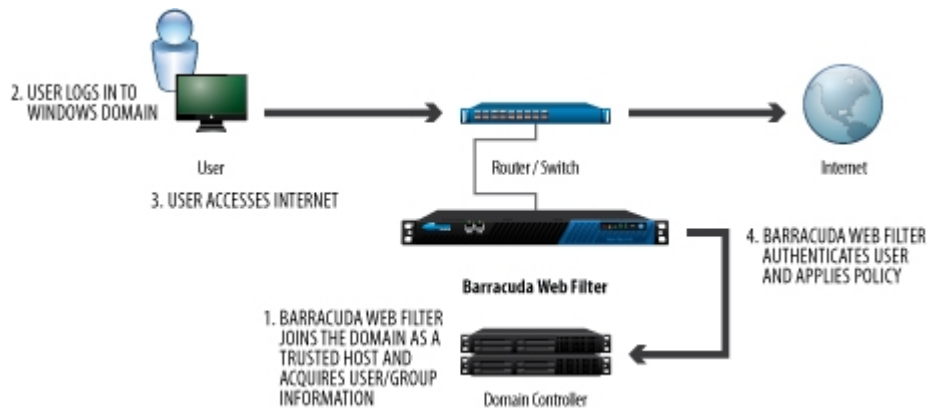


Figure 3. NTLM/Kerberos Authentication