How to Choose Your Authentication Mechanisms

https://campus.barracuda.com/doc/6160474/

This article presents some use case scenarios to help you decide which authentication scheme(s) to configure on your Barracuda Web Security Gateway. Each example addresses a particular type of environment. Note that LDAP authentication supports *multiple* domains on one Barracuda Web Security Gateway, but NTLM and Kerberos authentication mechanisms only support *one* domain per Barracuda Web Security Gateway.

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, FTP/FTPS, or SMB servers. Barracuda Networks 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.

Example 1: Fat clients (standard desktops) using Active Directory

Step 1: Configure **LDAP authentication**, as described in How to Enable LDAP Domain User Authentication, on the Barracuda Web Security Gateway and synchronize group membership information with your domain controllers (Active Directory servers). This provides a manual way for users to authenticate on the Barracuda Web Security Gateway so you can track user browsing activity.

Step 2: If you want to use single sign-on, install and configure the DC Agent on every domain controller as described in How to Get and Configure the Barracuda DC Agent. For an overview, see About the Barracuda DC Agent.

Example 2: Using only Citrix or other terminal environments

Step 1: Configure NTLM or Kerberos so that the Barracuda Web Security Gateway can join the domain. Reasons for choosing NTLM versus Kerberos are discussed below.

Step 2. Force users to use the Barracuda Web Security Gateway as a proxy server that provides authentication and single sign-on. See Forward Proxy Deployment of the Barracuda Web Security Gateway for details on proxy deployment.

Example 3: Mix of fat clients and Citrix or other terminal environments

Configure per examples 1 and 2. The articles in this section, linked above, further explain reasons and requirements for employing these various authentication schemes.

Exempting selected LDAP domain users from filtering

To exempt LDAP domain users from policy engine processing, on the **USERS/GROUPS > Authentication LDAP** tab, navigate to the **DC Agent Configuration** section where exempt user names can be entered. An example use case for this feature is to prevent traffic caused by script logic or other background users from appearing in the traffic log.

NTLM Versus Kerberos

Kerberos is an authentication protocol that provides mutual authentication; i.e. both the user and the server verify each other's identity. For this reason, Kerberos is considered a more secure authentication protocol than NTLM. Implementing Kerberos-based authentication within your network will allow the Barracuda Web Security Gateway to associate outgoing web requests with Active Directory users, log user activity, and apply user-specific or group-specific policies to outgoing connections without requiring users to log into the Barracuda Web Security Gateway.

Kerberos is useful when a Microsoft domain controller is running in native mode. It is a Forward Proxy authentication scheme and the Barracuda Web Security Gateway need not verify each authentication request against a domain controller. See How to Configure Kerberos Authentication for more information about Kerberos.

If your network uses an NT LAN Manager (**NTLM**) authentication server, your NTLM domain users transparently become authenticated in the Barracuda Web Security Gateway using their Microsoft Windows credentials. This single sign-on (SSO) method of access control is provided by transparent proxy authentication against the your NTLM server.

To enable transparent proxy authentication against your NTLM server, you must join the Barracuda Web Security Gateway to the NTLM domain as an authorized host. The process of joining the domain also synchronizes NTLM group information from your domain controller to the Barracuda Web Security Gateway. Configure NTLM authentication on the **USERS/GROUPS > Authentication** page **NTLM** tab. See How to Enable NTLM Domain User Authentication for more information about NTLM.