How to Configure Kerberos Authentication

https://campus.barracuda.com/doc/6160442/

Windows platforms use Kerberos as the native authentication method. Note that Kerberos is not supported for multiple domains on one Barracuda Web Security Gateway.

When to use Kerberos Authentication

Use Kerberos with the Barracuda Web Security Gateway in any of the following scenarios:

- **Clients are behind a NAT-enabled router** — Requests from users on client machines behind a NAT-enabled router would appear to the Barracuda Web Security Gateway to be sent from the same reusable NAT Router IP address.
- **Windows Terminal Services** — Requests from users using Windows Terminal Services to access remote data and applications on another client machine would appear to the Barracuda Web Security Gateway to be sent from the Windows terminal IP address.
- **Citrix Presentation Services** — Requests from users accessing remote data and applications on a Citrix Presentation Server would appear to the Barracuda Web Security Gateway to be sent from the Citrix Presentation Server.

Requirements for using a Kerberos authentication server

Before you integrate with a Kerberos authentication server, please verify the following requirements:

- The Barracuda Web Security Gateway is typically deployed as a forward proxy when using Kerberos authentication. However, in certain use cases where the Barracuda Web Security Gateway is deployed inline, traffic from users who authenticate via Kerberos can be proxied to the Barracuda Web Security Gateway. A common scenario for this use case is transitioning from one deployment/configuration to another, where some users are on a Citrix server, for example, and other users are on desktops using LDAP authentication. LDAP is the only other authentication service you may configure when using Kerberos authentication with the same Barracuda Web Security Gateway. This is called **Hybrid Authentication**.
  For more information on deploying your Barracuda Web Security Gateway as a forward proxy, please refer to Forward Proxy Deployment of the Barracuda Web Security Gateway.
- No Barracuda DC Agents are required if only using Kerberos authentication, but will be required if using LDAP authentication in addition to Kerberos.
- Web browsers must support Kerberos and must be configured to use the Barracuda Web Security Gateway as an HTTP proxy via port 3128.
- Client workstations and the Barracuda Web Security Gateway must have properly configured

DNS resolution mechanisms. DNS servers must be able to resolve IP addresses in both forward and reverse.
- All host machine clocks must be synchronized within 5 minutes of the Kerberos server clock.
- All users must have domain logon credentials, generally speaking; however, non-domain machines can use Kerberos authentication provided that Kerberos is configured correctly on those machines.

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.

Implementing Kerberos

Follow these steps to create your Kerberos service on the Barracuda Web Security Gateway:

1. Set your **Default Domain** and **Default Hostname** on the **BASIC > IP configuration** page. On your DNS server(s), add an entry (both forward and reverse mappings) for your Barracuda Web Security Gateway.
2. On the **Kerberos** tab of the **USERS/GROUPS > Authentication** page, enter the **Realm**, or Windows administrative domain name.
3. On that page, in the **KDC** field, enter the fully qualified domain name (FQDN) of the Key Distribution Center server for the realm you specified. This is typically the FQDN of your domain controller.
4. Enter the **Username** and **Password** of an account that has the minimum privileges required for access to your Active Directory server, as stated above. Do not include the domain name in the **Username** entry. For example, if the **Username** is *administrator*, simply enter **administrator**.
5. Click the **Add** button to create the new Kerberos service. Once you do this, the service should appear as type **Kerberos** in the **Existing Authentication Services** table on the **USERS/GROUPS > Authentication** page on the **Kerberos** tab.
6. Ensure that the Barracuda Web Security Gateway's FQDN (not the IP) and port 3128 are configured as an HTTP proxy on all users' browsers.

Important

If you have installed the **Barracuda DC Agent** software on your domain controller(s) for use with clients authenticating via LDAP, (see About the Barracuda DC Agent) make sure to do the following when adding users in terminal environments who will be authenticating with either Kerberos or NTLM:

1. Run the **Barracuda DC Agent** monitor and click on the **Filters** tab.
2. Specify any IP addresses for which the DC Agent **should not** capture and send login information (for LDAP logins) to your Barracuda Web Security Gateway. This includes Citrix or other terminal servers used when implementing Kerberos or NTLM authentication mechanisms, while you also have PCs using LDAP and utilize a Barracuda DC Agent. These IP addresses are exceptions and associated login events (for LDAP logins) will be ignored by the Barracuda DC Agent.

Note that implementing Kerberos Authentication will restrict some configuration options, as follows:

- **No login override of blocked pages**: When a policy on the Barracuda Web Security Gateway blocks Internet access for a user, that user will not be offered login fields at the bottom of the block message page, even if **Allow Login Override of Blocked Pages** is enabled on the **BLOCK/ACCEPT > Configuration** page.
- **No logout option**: Users cannot log out when proceeding to a blocked page in order to surf anonymously. More precisely, when a policy on the Barracuda Web Security Gateway blocks Internet access for user, that user will not be offered a logout option at the bottom of the block message page, even if the **Offer Logout** option on the **BLOCK/ACCEPT > Configuration** page is enabled.
- Users are not displayed in the **USERS/GROUPS > Account View** page when authenticated via Kerberos.

About Kerberos Authentication

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.