How to Configure Multi-Domain Kerberos Authentication

https://campus.barracuda.com/doc/41106101/

To set up multi-domain Kerberos authentication, add domains to the Kerberos authentication service on the **ACCESS CONTROL > Authentication Services** page. You can add a maximum of ten (10) domains to the Kerberos authentication service. If the domain name is appended with a user name, the user's credentials are validated with that domain for authentication. If the user fails to append the domain name, the user is authenticated using the default Kerberos database configured for that service.

Prerequisites

- You must create a one-way *forest level trust* between the domains. For more information, refer to the Microsoft article Creating Forest Trusts.
- Configure a DNS server to resolve the domain names from all domains that are in the multi-domain setup. If there are two (2) DNS servers in each of the domains, then configure DNS conditional forwarders in each DNS namespace to route the queries for names in other namespaces. For more information, refer to the Microsoft article Configure a DNS Server to Use Forwarder.

Configure the Barracuda Web Application Firewall for Multi-Domain Authentication

Perform the following steps to set up multi-domain Kerberos authentication:

1. Go to the **ACCESS CONTROL > Authentication Services** page.
2. Click the **KERBEROS** tab, enter the details of your Kerberos authentication server, enter the Domain Alias, and then click **Add**.
3. In the **Existing Authentication Services** section, click **Add** next to the Kerberos authentication service you created. The **Add Domain to Kerberos Service** window appears.
4. In the **Add Domains to Kerberos Service** window, enter the details of the domain and click **Add**.
5. Repeat Step 3 and 4 to add more domains.

Configuration Example for Multi-Domain Kerberos Authentication

As an example, consider that you have two (2) domains: "server.nc.com" and "users.nc.com", and both domains have users. The web server is under the "server.nc.com" domain and the users in the "users.nc.com" domain need access to "server.nc.com" domain.

1. Create one-way trust between the domains "server.nc.com" and "users.nc.com".
2. Ensure that all subdomains belonging to the domains are resolvable through the configured DNS server.

3. In the Barracuda Web Application Firewall web interface:
    1. In the **ACCESS CONTROL > Authentication Services** page, **KERBEROS** tab, use the "server.nc.com" domain details and create a Kerberos authentication service.
    2. On the same page in the **Existing Authentication Service** section, click **Add** next to the Kerberos authentication service you created in Step 3a.
    3. In the **Add Domain To Kerberos Service** window, enter the details of the "users.nc.com" domain and click **Add**.