Proxy authentication with Kerbeors ticket

In network structures where the user administration of TightGate-Pro is carried out via Active Directory (AD), it is possible to use the tickets created by AD to authenticate to uplink proxies. Of course, this is only possible if the proxy supports a ticket-based login. The following instructions describe the requirements and the procedure for AD authentication on a proxy.

Prerequisite:

- Only proxies are supported that use the following authentication protocol **Kerberos** as the authentication protocol. The outdated NTLM protocol is not supported.
- TightGate-Pro must have a functioning AD connection.
- AD authentication on the proxy is only possible with the Mozilla Firefox browser. The optional Chrome browser cannot currently be used for proxy authentication.
- For AD authentication on the proxy to be successful, the Mozilla Firefox browser must communicate directly with the proxy. This means that TightGate-Pro **does not log** and also **filtering** as both are done via an internal proxy.
- Every user ID that is to authorise itself at the proxy via AD ticket must be entered in the AD security group **tgunfiltered** in the AD security group.
- Kerberos delegation for tickets must be permitted in AD for the computer account of TightGate-Pro.

This is how it works:

- Login to TightGate-Pro as administrator ***config*** and call up the menu item **proxy**.
- Select the menu item **HTTP proxy** menu item and enter the name of the proxy to which the AD authentication is to take place.
  Attention: The name of the proxy must be used and it must be resolvable. Using an IP address will not work.
- In the menu item **HTTP proxy port** menu item, enter the port via which the proxy is addressed.
- In the menu item **HTTP proxy network** menu item, enter the IP address of the proxy. If several proxies are used, the proxy network must be entered in the form IP/Valid Bits.
- In the menu item **Proxy exceptions** menu item, enter two exceptions. On the one hand the **IP of the proxy** and secondly the **name of the proxy** secondly. It is absolutely necessary to define the IP address and the name of the proxy as exceptions.
- Under the menu item **AD/Kerberos proxy login** is **Yes** must be selected.
- In the menu item **AD/Kerberos proxy service** the value **HTTP** unless a different service is used.
- In the menu item **AD/Kerberos-Proxy-Realm** menu item, enter the REALM of the proxy if it differs from the REALM of the AD. Otherwise, the field can be left empty.
- Finally, save the settings **Save** and **Apply**.

Finished.