Network

The network interfaces and the accessible servers are configured in this menu. An overview of all menu options is provided below:

Menu item	Description
Network Interfaces	Configuration of the network interfaces available in TightGate-Pro. The settings must be made according to the operating environment.
Enable IPv6	Activates or deactivates Iv6 support in TightGate-Pro. Even without activation at this point, IPv6 addresses can be entered for all IP addresses in TightGate-Pro. However, these are only used if IPv6 support has been activated at this point.
—	
Name Servers*	IPv4 address of a name server (DNS) for resolving IPv4 addresses. Up to 25 name servers can be referenced. They are requested in the order of the entries if individual servers cannot be reached.
Local Domain Servers*	Definition of locally used domains and the associated name servers. This setting is particularly important for Active Directory connections if the AD server cannot/may not perform DNS resolution on the Internet. **Caution:** As a rule, the reverse resolution (IPv4 address → DNS name) must also be specified in a separate entry.
Time Server*	IPv4 address of a time server for obtaining the system time. Up to 25 time servers can be referenced. These are requested in the order of the entries if individual servers are not available. **Warning:** The correct system time across all nodes is particularly important in a cluster network. Time differences between the computers in a cluster can lead to malfunctions. It is therefore essential to ensure that at least one time server is always available. It is recommended to use the same time server that is used by the Active Directory server.
—	
Client Local Networks*	IPv4 addresses or address ranges that are authorised to connect to TightGate-Pro. If a special gateway is required for a client network, this must be specified directly in the form [IP address/valid bits/gateway]. A maximum of 25 client networks can be defined. **Note:** Access from TightGate-Pro to services/servers located in client networks is generally prohibited. **Caution:** The client network must not be defined with the address range 0.0.0.0/0, as otherwise Internet access is not possible.
Privileged Clients*	The IPv4 addresses that are to receive privileged access to TightGate-Pro must be entered here. TightGate-Pro The licence distinguishes between two limits up to which user logins are permitted. These are defined in the licence of TightGate-Pro. The first limit is the number of regular users, the second limit is the number of privileged users. As soon as the number of authorised regular users is reached, only privileged users are permitted - provided their number has not yet been reached. Once the second limit has been reached, any further attempt by a client to connect to TightGate-Pro is rejected with a corresponding error message. Privileged clients are not only authorised according to a separate quota, but are also allocated a larger share of working and mass memory as well as CPU time on TightGate-Pro. **Note:** Privileged clients can also be set up based on the user ID. This is done in the user administration as administrator ***maint***.

Menu item	Description
Mail server*	All relevant settings for e-mail functionality for users are summarised under this menu item for the sake of clarity. This includes the setting of the mail domain as well as the default for POP3/IMAP and SMTP.
Admin Networks*	Definition of IP addresses or IP network areas that allow administrative access (for the roles ***config, maint, update, backuser, root*** and ***security***) to TightGate-Pro. If a network is configured here, the following menu item appears, under which the port for administrative access via SSH can be defined.
Admin SSH port*	Selection of the alternative SSH port via which the administration networks gain access to TightGate-Pro. Ports 22,222,2222 and 22222 are available for selection. **Caution:** If you make a setting that differs from the standard port 22, please ensure that the firewall rules for accessing the administration networks are set correctly in your network.
Nagios/SNMP Networks*	Specification of all IP addresses of monitoring servers that are to monitor TightGate-Pro. For monitoring, the respective service (NRPE/SNMP) must be activated under the Services to enable monitoring.
SSH Out*	IPv4 addresses of SSH servers that can be accessed directly via TightGate-Pro. The servers must be specified in the form [IP address/valid bits]. A maximum of 25 SSH servers (or networks) are permitted.
HTTP Out*	IPv4 addresses of the HTTP servers that can be accessed directly (without proxy) via TightGate-Pro. The servers must be specified in the form [IP address/valid bits]. A maximum of 25 HTTP servers (or networks) are permitted. **Caution:** If under **Proxy > Proxy exceptions** servers are defined under Proxy > Proxy exceptions, these must also be explicitly entered here, as otherwise the servers may not be accessible.
HTTP Ports*	Specifies the ports to which the servers defined under **HTTP server** may connect to. **Note:** This menu item is only available if HTTP servers are entered.
RDP/Citrix Out*	IPv4 address(es) of Citrix or Windows servers that can be accessed directly from TightGate-Pro. A corresponding client programme (remmina) is already implemented in TightGate-Pro. Its use is described in the user manual under Remote Desktop Connections to CITRIX and Windows Servers.