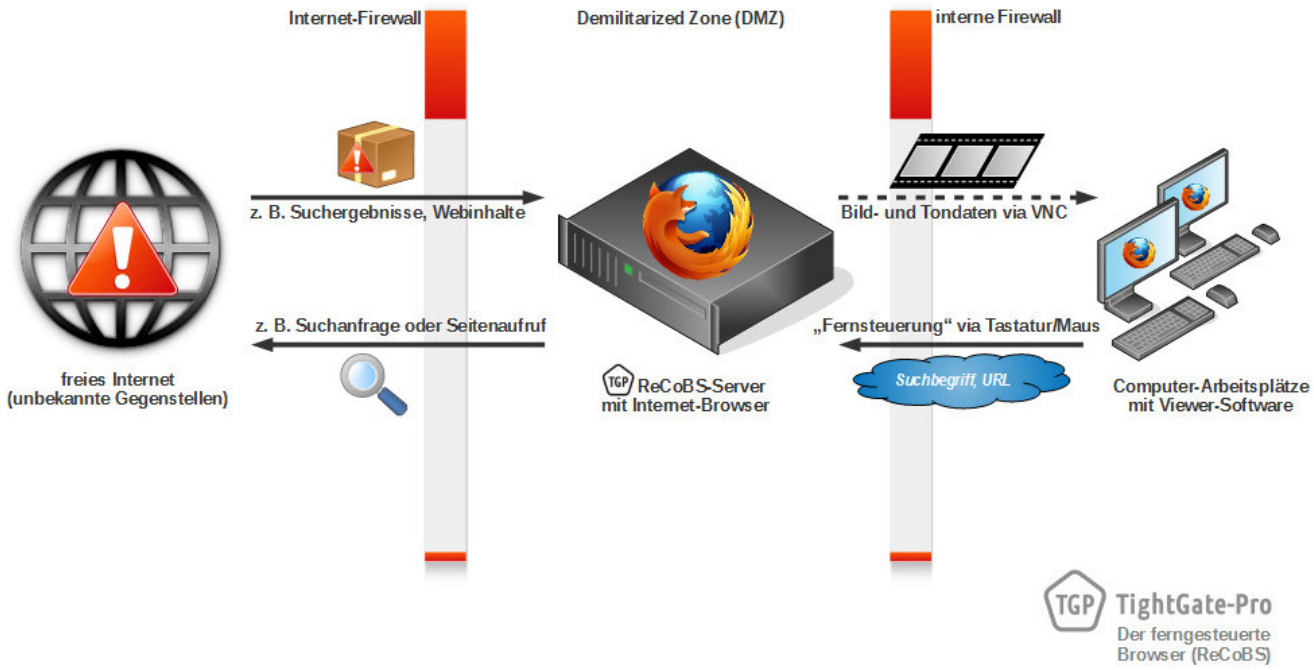
Network specifications and connection paths

The following overview shows the ports and protocols that are required for TightGate-Pro to be operated in the network. The internal firewall (packet filter or layer 3 switch) shown must be provided by the operator.



Firewall settings

TightGate-Pro is generally intended for operation in a demilitarised zone (DMZ). It must be ensured that client computers in the internal network only connect to TightGate-Pro via the designated ports. Furthermore, direct Internet access by bypassing TightGate-Pro must be prevented using suitable firewalls or packet filters.

Connection paths that are not absolutely necessary for the proper operation of TightGate-Pro are marked as "optional" and should be deactivated if the functionality realised via them is not required.

Outgoing connections

For UDP connections, associated UDP response packets in the opposite direction must also be enabled.

Sender	Destination	Protocol	Port(s)	Remark	Optional
TightGate-Pro	Internet	TCP	80, 443 or specific proxy port	Access for HTTP(S) connections to the Internet. If a proxy is connected upstream, the connection to the proxy must be enabled.	
TightGate-Pro	m-privacy Update server TCP 22 or 443 or proxy SSH access via port 443 or 22 to update server of			m-privacy GmbH **Attention:** See also the configuration settings for the update.	
TightGate-Pro	Internet	UDP	80, 443, 1024:65535	Requests from WebRTC services such as Webex or Zoom. Webmeeting services may require additional network shares. These may vary depending on the application.	X
TightGate-Pro	specific	UDP	123	Requests to time servers	X
TightGate-Pro	specific	TCP + UDP	53	Requests to name servers	X
TightGate-Pro	specific	TCP	25	Further authorisations required if e-mail services are to be used via TightGate-Pro: POP3: 110 - POP3/SSL: 995 IMAP4: 143 - IMAP4/SSL: 993	X
TightGate-Pro	specific	TCP + UDP	88	Communication with Active Directory	X
TightGate-Pro	specific	TCP	389,636 3268,3269	Communication with Active Directory (LDAP / LDAPS) Queries to determine a global catalogue	X
TightGate-Pro	specific	TCP	21, 22	Direct access to server via FTP, SFTP/SSH	X
TightGate-Pro	specific	TCP + UDP	514, 2514, 3514	Configurable ports for sending syslog messages to central syslog servers . for sending syslog messages to central syslog servers. (Syslog / RELP / RELPTLS)	X
TightGate-Pro	specific	TCP UDP	3389, 1494, 80, 443 1604	RDP or CITRIX server incoming and outgoing	X

Incoming connections (LAN)

Originator	Destination	Protocol	Port(s)	Remark	Optional
Clients (workstation PC)	TightGate-Pro	TCP	5900	TLS-encrypted connection of the TightGate-Viewers to TightGate-Pro.	
Clients (workstation PC)	TightGate-Pro	TCP	22	SFTP-encrypted connection to use the file lock of TightGate-Pro.	X
Administration network	TightGate-Pro	TCP	222 2222 22222	SSH access for the administration of TightGate-Pro. One of the ports can be set. If none of the ports is selected, administrative access is via port 22.	X

Incoming connections (DMZ/Internet)

Sender	Destination	Protocol	Port(s)	Remark	Optional
Internal DNS service	TightGate-Pro Cluster system	UDP TCP	53	These ports are only to be released if a TightGate-Pro cluster is used. For responses that exceed the packet size of UDP, TCP port 53 must be released.	X
Monitoring with SNMP	TightGate-Pro	UDP	161	SNMP requests	X
Monitoring with NRPE	TightGate-Pro	TCP	5666	Access from ZenTiV or other NRPE-based monitoring systems	X