

# Network specifications and connection paths

The following overview describes all ports and protocols that are required for the operation of TightGate-Pro in the network. An internal firewall (packet filter or layer 3 switch) must be provided by the operator.



## Firewall settings

TightGate-Pro is designed for use in a demilitarised zone (DMZ). It must be ensured that workstations in the internal network only connect to TightGate-Pro via the designated ports. In addition, suitable firewall or packet filter rules must be used to prevent internal systems from reaching the Internet directly by bypassing TightGate-Pro.

Connection paths that are not required for regular operation must be marked as **optional** labelled as optional. They should be deactivated if the corresponding functions are not used.

## Outgoing connections

### Hinweis

For UDP connections, the associated response packets must also be authorised.

Sender	Destination	Protocol	Port(s)	Remark	Optional
TightGate-Pro	Internet	TCP	80, 443 or proxy port	HTTP(S) access to the Internet. If a proxy is connected upstream, its port must be released.	
TightGate-Pro	m-privacy Update server	TCP	22 or 443 or proxy	m-privacy GmbH See: <a href="#">Configuration settings for the update.</a>	
	SSH access to the update servers of .				

Sender	Destination	Protocol	Port(s)	Remark	Optional
TightGate-Pro	Internet	UDP	80, 443, 1024:65535	Use of WebRTC services (e.g. Webex, Zoom). Depending on the provider, further authorisations may be required. See: <a href="#">List of supported web meeting platforms</a> .	X
TightGate-Pro	specific	UDP	123	NTP requests	X
TightGate-Pro	specific	TCP + UDP	53	DNS queries	X
TightGate-Pro	specific	TCP	25	For e-mail use: POP3: 110 / POP3-SSL: 995 / IMAP4: 143 / IMAP4-SSL: 993	X
TightGate-Pro	specific	TCP + UDP	88	Kerberos communication	X
TightGate-Pro	specific	TCP	389,636 3268,3269	LDAP/LDAPS and queries of the global catalogue	X
TightGate-Pro	specific	TCP	22, specific	Direct access to SSH or HTTP server	X
TightGate-Pro	specific	TCP + UDP	514,2514,3514	Configurable ports for Syslog/RELP/RELP-TLS. See: <a href="#">Playing out syslog messages to central syslog servers</a> .	X
TightGate-Pro	specific	TCP UDP	3389,1494,80,443 1604	Communication with RDP or Citrix servers (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 access for the file transfer.	X
Administration network	TightGate-Pro	TCP	222 2222 22222	SSH access for administration. If no admin port is selected, 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	Only required when using a cluster. TCP-53 is required if responses exceed the maximum UDP packet size.	X
SNMP monitoring	TightGate-Pro	UDP	161	SNMP requests	X
NRPE monitoring	TightGate-Pro	TCP	5666	Access from ZenTiV or other NRPE-based monitoring systems	X

From:  
<https://help.m-privacy.de/> -

Permanent link:  
<https://help.m-privacy.de/doku.php/en:tightgate-pro:einfuehrung:informationen>

Last update: **2025/12/04 10:51**

