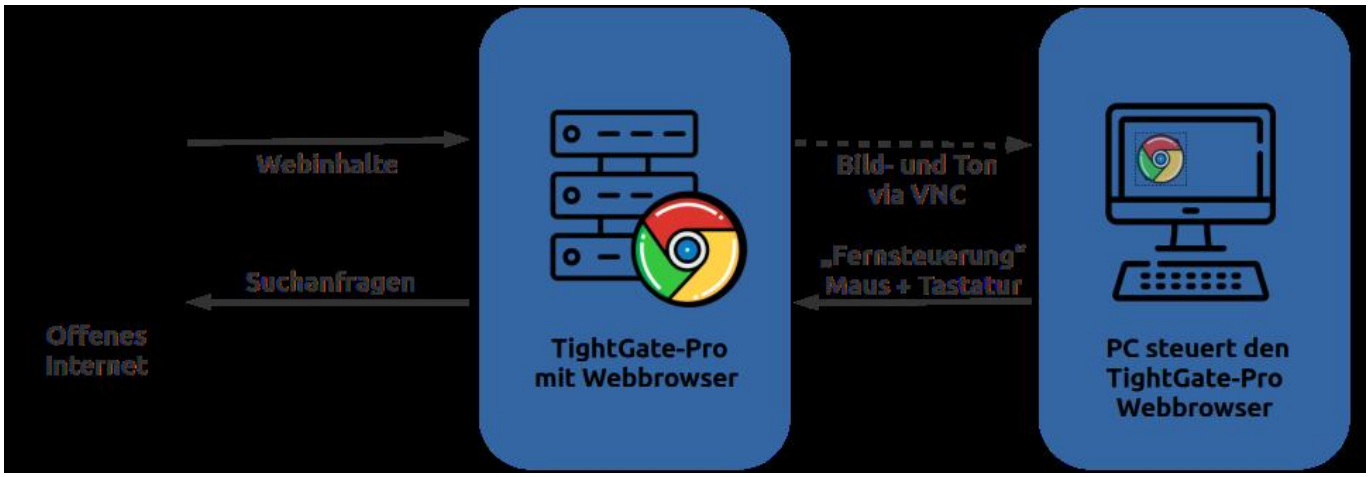
Netzwerkvorgaben und Verbindungswege

Die folgende Übersicht beschreibt sämtliche Ports und Protokolle, die für den Betrieb von TightGate-Pro im Netzwerk erforderlich sind. Eine interne Firewall (Paketfilter oder Layer-3-Switch) muss vom Betreiber bereitgestellt werden.



Firewall-Einstellungen

TightGate-Pro ist für den Einsatz in einer Demilitarisierten Zone (DMZ) konzipiert. Es ist sicherzustellen, dass sich Arbeitsstationen im internen Netzwerk ausschließlich über die vorgesehenen Ports mit TightGate-Pro verbinden. Zudem muss durch geeignete Firewall- oder Paketfilterregeln verhindert werden, dass interne Systeme das Internet unter Umgehung von TightGate-Pro direkt erreichen.

Nicht für den regulären Betrieb benötigte Verbindungswege sind als **optional** gekennzeichnet. Sie sollten deaktiviert werden, sofern die entsprechenden Funktionen nicht genutzt werden.

Ausgehende Verbindungen

Hinweis

Bei UDP-Verbindungen müssen die zugehörigen Antwortpakete ebenfalls zugelassen werden.

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
TightGate-Pro	Internet	TCP	80, 443 oder Proxy-Port	HTTP(S)-Zugriff ins Internet. Bei vorgeschaltetem Proxy ist dessen Port freizugeben.	
TightGate-Pro	m-privacy Update-Server	TCP	22 oder 443 oder Proxy	SSH-Zugriff auf die Update-Server der m-privacy GmbH. Siehe: Konfigurationseinstellungen für das Update.	

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
TightGate-Pro	Internet	UDP	80, 443, 1024:65535	Nutzung von WebRTC-Diensten (z. B. Webex, Zoom). Je nach Anbieter können weitere Freigaben erforderlich sein. Siehe: Liste unterstützter Webmeeting-Plattformen.	X
TightGate-Pro	spezifisch	UDP	123	NTP-Anfragen	X
TightGate-Pro	spezifisch	TCP + UDP	53	DNS-Abfragen	X
TightGate-Pro	spezifisch	TCP	25	Für E-Mail-Nutzung: POP3: 110 / POP3-SSL: 995 / IMAP4: 143 / IMAP4-SSL: 993	X
TightGate-Pro	spezifisch	TCP + UDP	88	Kerberos-Kommunikation	X
TightGate-Pro	spezifisch	TCP	389,636 3268,3269	LDAP/LDAPS sowie Abfragen des Globalen Katalogs	X
TightGate-Pro	spezifisch	TCP	22, spezifisch	Direkter Zugriff auf SSH- oder HTTP-Server	X
TightGate-Pro	spezifisch	TCP + UDP	514,2514,3514	Konfigurierbare Ports für Syslog/RELP/RELP-TLS. Siehe: Ausspielen von Syslog-Meldungen an zentrale Syslog-Server.	X
TightGate-Pro	spezifisch	TCP UDP	3389,1494,80,443 1604	Kommunikation mit RDP- oder Citrix-Servern (ein- und ausgehend)	X

Eingehende Verbindungen (LAN)

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
Klienten (Arbeitsplatz-PC)	TightGate-Pro	TCP	5900	TLS-Verschlüsselte Verbindung des TightGate-Viewers zu TightGate-Pro.	
Klienten (Arbeitsplatz-PC)	TightGate-Pro	TCP	22	SFTP-Zugriff für die Dateischleuse.	X
Administrationsnetzwerk	TightGate-Pro	TCP	222 2222 22222	SSH-Zugriff für Administration. Falls kein Admin-Port gewählt wird, erfolgt der Zugriff über Port 22.	X

Eingehende Verbindungen (DMZ/Internet)

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
Interner DNS-Dienst	TightGate-Pro Clustersystem	UDP TCP	53	Erforderlich nur bei Verwendung eines Clusters. TCP-53 wird benötigt, wenn Antworten die maximale UDP-Paketgröße überschreiten.	X
SNMP-Monitoring	TightGate-Pro	UDP	161	SNMP-Anfragen	X

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
NRPE-Monitoring	TightGate-Pro	TCP	5666	Zugriff von ZenTiV oder anderen NRPE-basierte Monitoring-Systeme	X