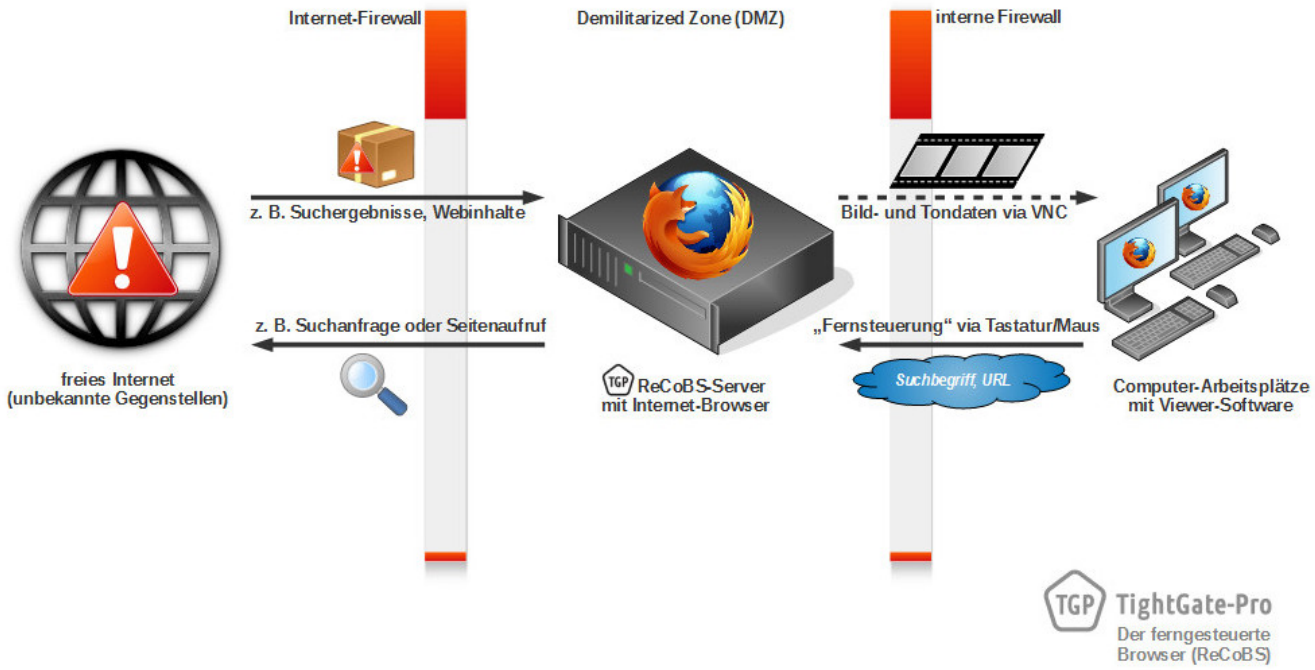
Netzwerkvorgaben und Verbindungswege

Die nachfolgende Übersicht zeigt die Ports und Protokolle auf, welche benötigt werden, damit TightGate-Pro im Netzwerk betrieben werden kann. Die eingezeichnete interne Firewall (Paketfilter oder Layer3-Switch) ist betreiberseitig zur Verfügung zu stellen.



Firewall-Einstellungen

TightGate-Pro ist grundsätzlich zum Betrieb in einer Demilitarisierten Zone (DMZ) vorgesehen. Es ist sicherzustellen, dass sich Klientenrechner im internen Netzwerk nur über die vorgesehenen Ports mit TightGate-Pro verbinden. Weiterhin ist durch geeignete Firewalls bzw. Paketfilter der direkte Internetzugriff unter Umgehung von TightGate-Pro zu unterbinden.

Nicht unbedingt für den ordnungsgemäßen Betrieb von TightGate-Pro erforderliche Verbindungswege sind als "optional" gekennzeichnet und sollten deaktiviert werden, sofern die hierüber realisierte Funktionalität nicht benötigt wird.

Ausgehende Verbindungen

Bei UDP-Verbindungen sind zugehörigen UDP-Antwortpakete in Gegenrichtung ebenfalls freizugeben.

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
TightGate-Pro	Internet	TCP	80, 443 oder spezifischer Proxy-Port	Zugriff für HTTP(S)-Verbindungen ins Internet. Sofern ein Proxy vorgeschaltet ist, ist die Verbindung zu dem Proxy freizugeben.	
TightGate-Pro	m-privacy Update-Server	TCP	22 oder 443 oder Proxy	SSH-Zugriff über Port 443 oder 22 auf Updateserver der m-privacy GmbH **Achtung:** Siehe dazu auch die Konfigurationseinstellungen für das Update.	
TightGate-Pro	Internet	UDP	80, 443, 1024:65535	Anfragen von WebRTC-Diensten wie Webex oder Zoom. Ggf. benötigen Webmeeting Dienste zusätzliche Netzwerkfreigaben. Diese können ja nach Anwendung variieren.	X
TightGate-Pro	spezifisch	UDP	123	Anfragen an Zeitserver	X
TightGate-Pro	spezifisch	TCP + UDP	53	Anfragen an Nameserver	X
TightGate-Pro	spezifisch	TCP	25	Weitere Freigaben erforderlich, falls E-Mail Dienste über TightGate-Pro genutzt werden sollen: POP3: 110 - POP3/SSL: 995 IMAP4: 143 - IMAP4/SSL: 993	X
TightGate-Pro	spezifisch	TCP + UDP	88	Kommunikation mit Active-Directory	X
TightGate-Pro	spezifisch	TCP	389,636 3268,3269	Kommunikation mit Active-Directory (LDAP / LDAPS) Abfragen zur Ermittlung eines Globalen-Katalogs	X
TightGate-Pro	spezifisch	TCP	21, 22	Direkter Zugriff auf Server per FTP, SFTP/SSH	X
TightGate-Pro	spezifisch	TCP + UDP	514, 2514, 3514	Konfigurierbare Ports für das Ausspielen von Syslog-Meldungen an zentrale Syslog-Server. (Syslog / RELP / RELPTLS)	X
TightGate-Pro	spezifisch	TCP UDP	3389, 1494, 80, 443 1604	RDP- bzw. CITRIX-Server 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-Verschlüsselte Verbindung zur Nutzung der Dateischleuse von TightGate-Pro.	X

Absender	Ziel	Protokoll	Port(s)	Bemerkung	Optional
Administrationsnetzwerk	TightGate-Pro	TCP	222 2222 22222	SSH-Zugriff zur Administration von TightGate-Pro. Es kann einer der Ports eingestellt werden. Wird keiner der Ports ausgewählt, erfolgt der administrative 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	Diese Ports sind nur freizugeben, sofern ein TightGate-Pro Cluster verwendet wird. Bei Antworten, die die Paketgröße von UDP überschreiten, ist der TCP-Port 53 freizugeben.	X
Monitoring mit SNMP	TightGate-Pro	UDP	161	SNMP-Anfragen	X
Monitoring mit NRPE	TightGate-Pro	TCP	5666	Zugriff von ZenTiV oder anderen NRPE-basierten Monitoring-Systemen	X