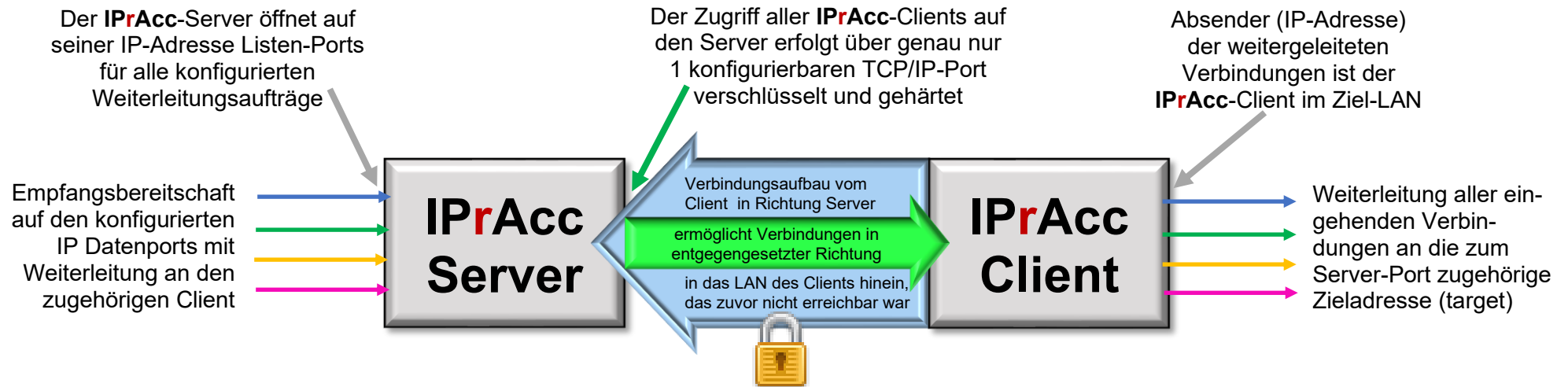


Grundfunktion

Alle **IPrAcc**-Clients bauen auf nur 1 konfigurierbaren Port eine permanente und überwachte TCP/IP-Verbindung zum **IPrAcc**-Server auf. Falls diese Verbindung unterbrochen wird, versuchen die Clients regelmäßig automatisch, diese Verbindung wieder herzustellen. Der gleiche Port wird auch für alle Datenverbindungen zwischen Clients und Server genutzt.

Im **IPrAcc**-Client werden alle gewünschten Weiterleitungsaufträge vom Server in das Client-LAN konfiguriert. Somit behält der Besitzer des Clients stets die Hoheit darüber, welche Verbindungen er in sein Netz zulässt.

Der Client meldet alle Weiterleitungsaufträge an den Server, der daraufhin die entsprechenden IP-Datenports auf seiner Seite öffnet:



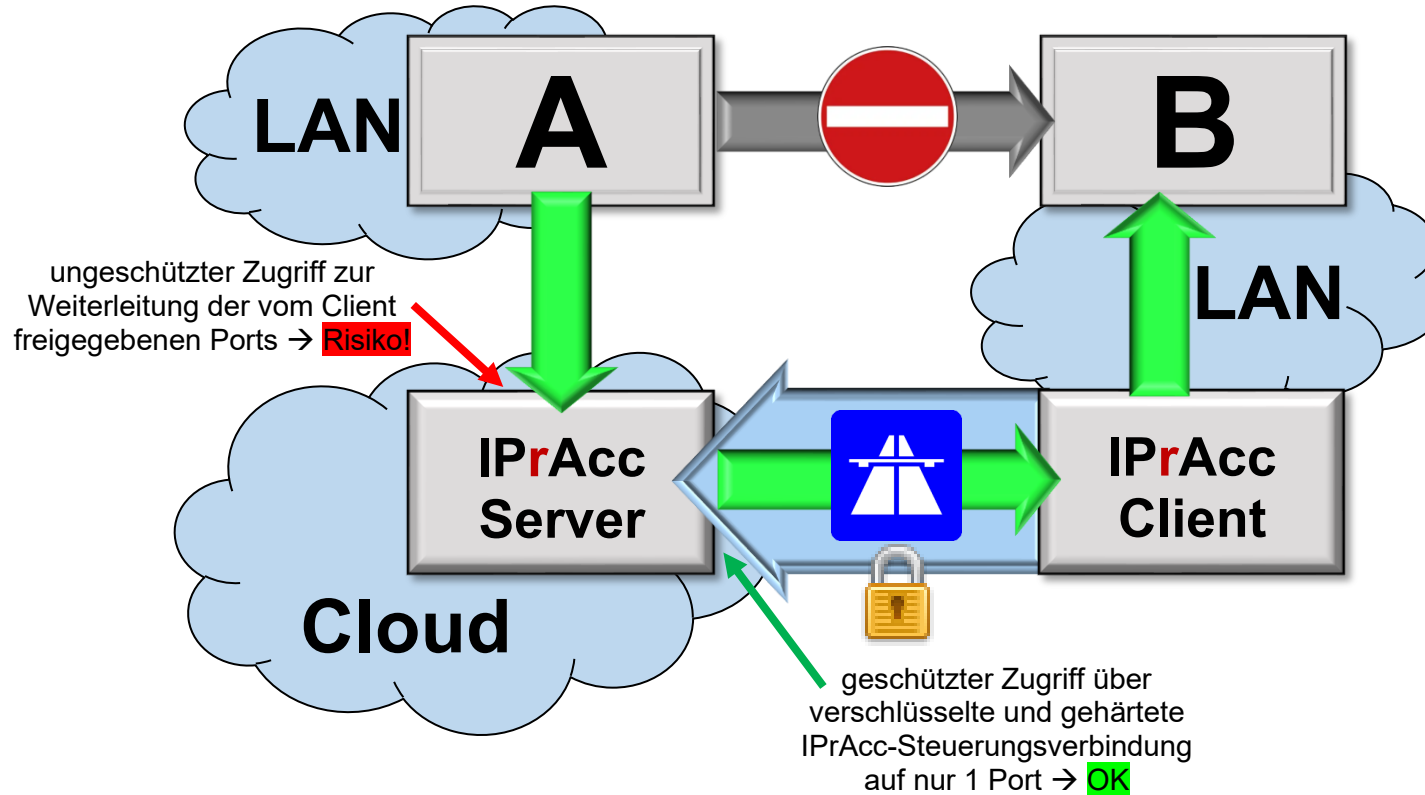
Alle Verbindungen zwischen **IPrAcc**-Clients und **IPrAcc**-Servern sollten stets verschlüsselt konfiguriert werden, damit die Daten bei der Übertragung vor dem Auslesen und Manipulieren geschützt sind.

Mehrere Clients können sich auf den gleichen Server verbinden. Somit kann beispielsweise eine Leitstelle, die einen **IPrAcc**-Server betreibt, darüber viele verschiedene Kunden (Clients) aufschalten.

„Server“ und „Client“ meint hier nicht Hardware, sondern Softwaremodule, die auf ggf. bereits vorhandenen PCs bei Bedarf auch mehrfach gestartet werden können. Damit lassen sich je nach Anforderungen und Anwendungsfall (use case) unterschiedliche Szenarien realisieren.

Szenario A

Der IPrAcc Server wird als **öffentlicher Server** in der Cloud betrieben (z.B. ebues-server.de):

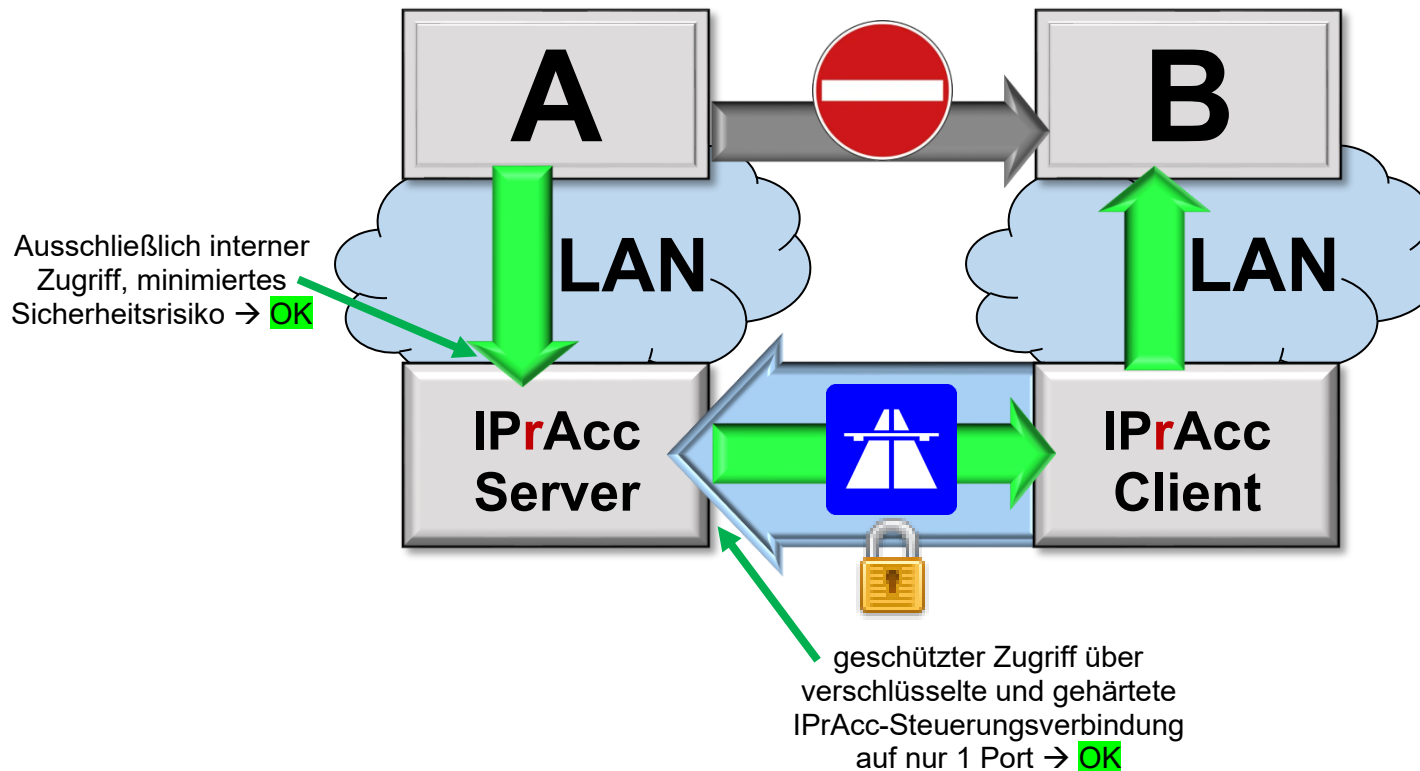


Das ermöglicht schnell und bequem einen Zugriff von allen Seiten, aber ACHTUNG - **Sicherheitsrisiko**: Auch Fremde können über den Server auf alle weitergeleiteten IP-Ports und somit alle konfigurierten Gegenstellen im LAN von B zugreifen!

Dieses Szenario ist deshalb nur zulässig, wenn alle damit weitergeleiteten Ports gegen öffentliche Zugriffe ausreichend gehärtet sind. Alternativ oder ergänzend können die Ports durch eine Whitelist in den Clients vor unbefugten Zugriffen geschützt werden.

Szenario B

Der **IPrAcc**-Server wird als **privater Server** im LAN A betrieben, nur 1 Port für den Zugriff der **IPrAcc**-Clients wird vom LAN A nach außen freigegeben, und diese Verbindung ist durch Verschlüsselung und die Eigenschaften des **IPrAcc**-Protokolls (Verbindungen, die sich nicht binnen 10 Sekunden korrekt authentifizieren, werden abgeworfen) gesichert:

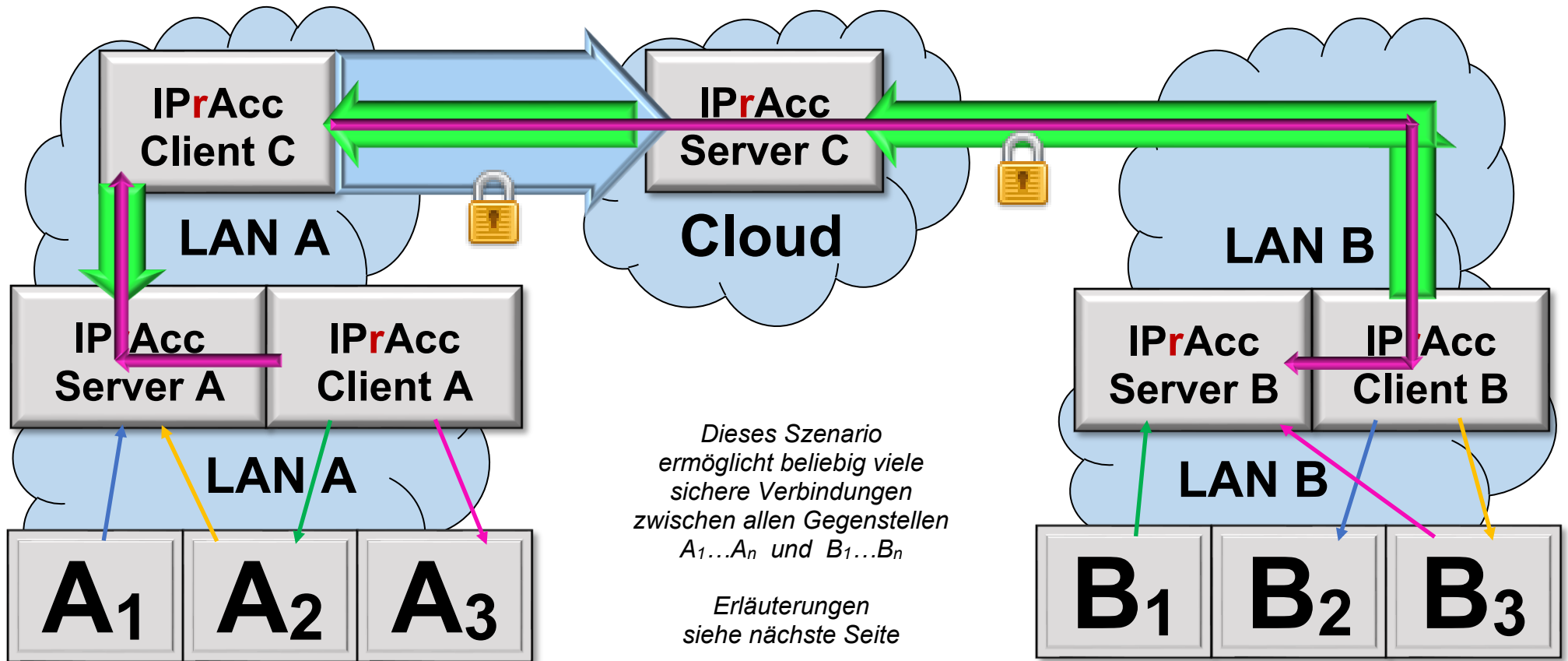


Dies ist sicherer, denn nun kann nur aus dem LAN A auf die weitergeleiteten Ports des **IPrAcc** Servers zugegriffen werden, und sämtliche Daten aller Verbindungen von A nach B werden außerhalb der LANs Dank **IPrAcc** verschlüsselt übertragen.

Szenario C

Als kleine Demonstration, was mit **IPrAcc** alles möglich ist, hier noch ein etwas komplexeres Szenario:

Wenn weder **LAN A** noch **LAN B** von außen erreichbar sind, aber dennoch zwischen beiden LANs in beiden Richtungen beliebig viele IP-Verbindungen zwischen allen Gegenstellen $A_1...A_n$ und $B_1...B_n$ aufgebaut werden sollen, kann ein **IPrAcc**-Server in der **Cloud** verwendet werden, der von beiden LANs aus erreichbar ist. Damit dabei alle Verbindungen sicher sind, kann folgendes Szenario konfiguriert werden:





Erläuterungen zu Szenario C

IPrAcc-Client C (C wie Cloud) stellt eine Verbindung zu **IPrAcc-Server C** her und baut damit die breite hellblaue Brücke. Die einzige Aufgabe von Client C besteht darin, Client B den Zugriff auf Server A zu ermöglichen. Dies ist deshalb leicht zu konfigurieren.

Der **IPrAcc-Server C** ist nur über einen gehärteten Port mit starkem Passwort erreichbar; somit kann kein Fremder darauf zugreifen. Client C lässt zusätzlich auf Server C nur den Zugriff auf **IPrAcc-Server A** über dessen gehärteten Steuerungs-Port zu; somit ist auch diese Verbindung vor fremden Zugriffen gut geschützt.

IPrAcc-Client B kann nun darüber eine Verbindung zu **IPrAcc-Server A** (im LAN A) aufbauen (hellgrüne Pfeile). Darüber können schon einmal alle Gegenstellen $A_1 \dots A_n$ sichere Verbindungen zu allen Gegenstellen $B_1 \dots B_n$ in LAN B aufbauen.

Damit auch sichere Verbindungen von LAN B ins LAN A möglich werden, verbindet sich nun noch **IPrAcc-Client A** über den gesicherten Pfad von Server A über Client B zu Server B (im LAN B).

Damit können nun auch alle Gegenstellen $B_1 \dots B_n$ Verbindungen zu allen Gegenstellen $A_1 \dots A_n$ in LAN A aufbauen.

Bei diesem Szenario gibt es nur genau 2 nach außen offene Ports:

- Steuerungs-Port von **IPrAcc-Server C**
- Steuerungs-Port von **IPrAcc-Server A**, freigegeben durch **IPrAcc-Client C** an **IPrAcc-Server C**

Diese beiden Ports sind durch das **IPrAcc-Protokoll** gehärtet und nur mit dem intern vereinbarten starken Passwort nutzbar. Es gibt keine anderen Zugriffsmöglichkeiten von außen auf dieses System. Alle übertragenen Daten werden auf ihrem kompletten Weg außerhalb der beiden LANs durchgängig verschlüsselt.

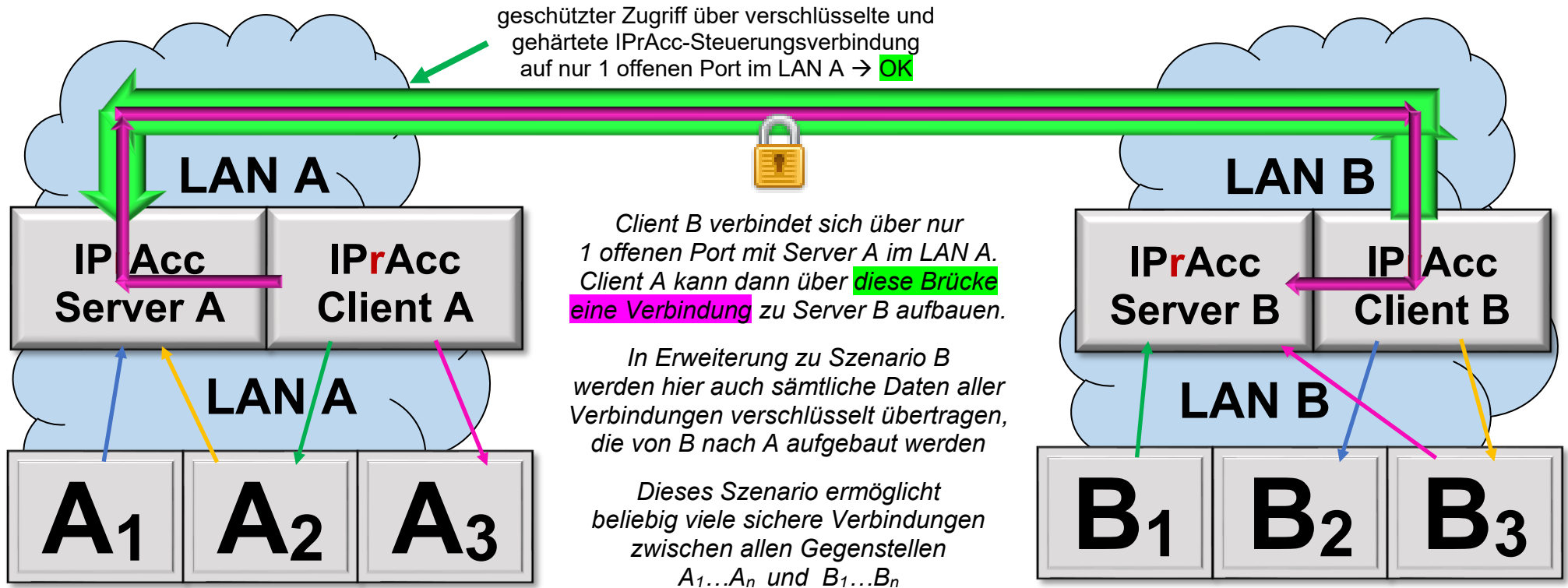
Server A bzw. B nehmen jeweils die Verbindungsanforderungen aus ihren LANs entgegen und leiten sie an den zuständigen Client weiter. Client B bzw. A geben diese Verbindungen dann zur konfigurierten Zieladresse (target: IP-Adresse und Port) in ihrem LAN weiter

Die Server und Clients jedes LANs können wahlweise über mehrere PCs verteilt oder auch alle gemeinsam auf 1 PC laufen, und dieser PC kann gleichzeitig auch Gegenstelle für weitere Verbindungen sein; die Zieladresse lautet dann localhost.

Bitte nicht erschrecken vor so vielen „Servern“: Die „Server“ sind genau wie die „Clients“ jeweils nur kompakte Anwendungen mit weniger als 10MB Umfang, die in wenigen Minuten auf jedem Windows-PC installiert und konfiguriert werden können.

Szenario D

Wenn ein **Direkter** Zugriff per IP von LAN B auf einen **Dedizierten** Server im LAN A (beispielsweise einer Leitstelle) ermöglicht werden kann, wird kein Server in der **Cloud** benötigt. Dann kann Szenario C zu Szenario D vereinfacht werden:



- **Ausgehende Verbindungen** werden von den Geräten A_i oder B_i über den im eigenen LAN verfügbaren **IPrAcc-Server** aufgebaut
- **Eingehende Verbindungen** werden von den **IPrAcc-Clients** innerhalb des jeweiligen LANs an die Zielgeräte B_i oder A_i weitergeleitet

Das funktioniert bei Szenario D in beiden Richtungen.

→ www.ipracc.com/support