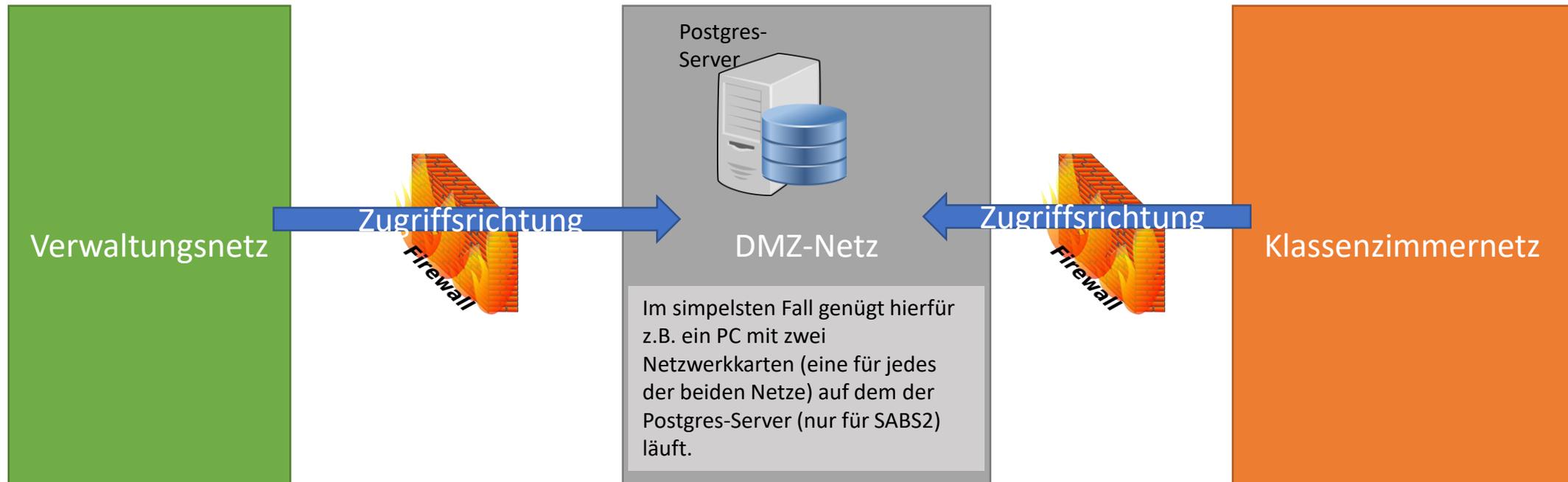


DMZ-Variante mit Windows-Client im Klassenzimmer

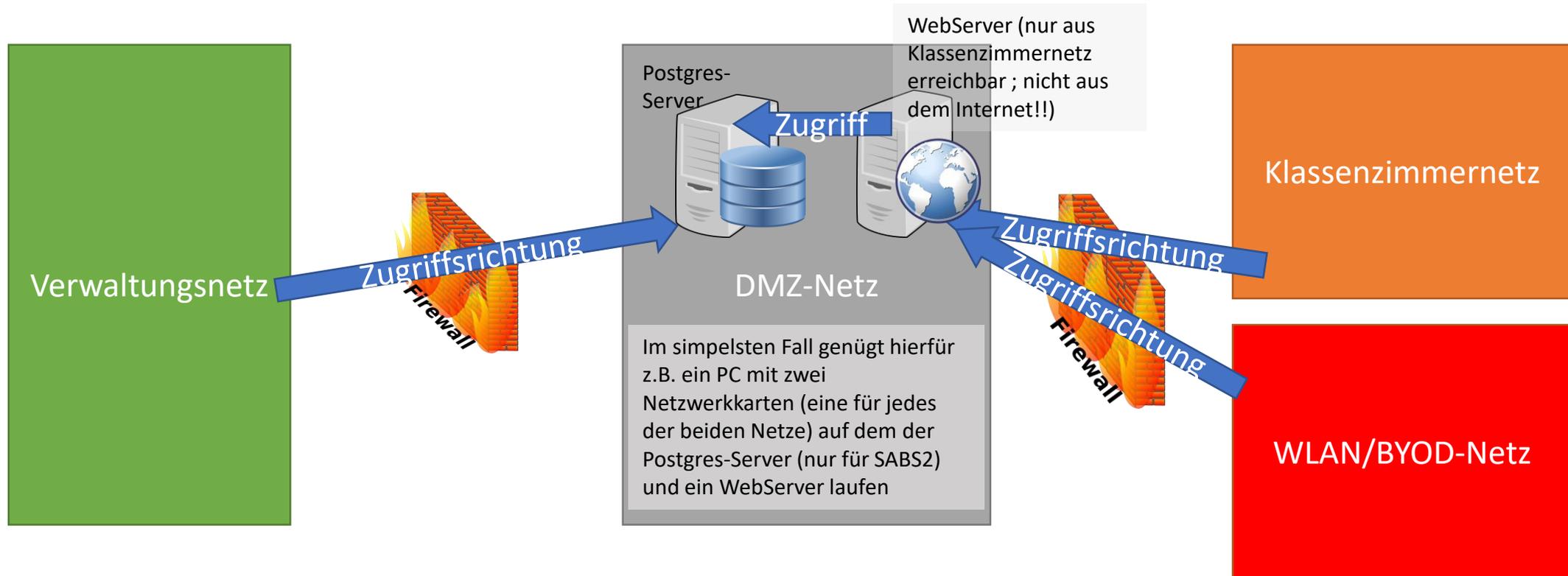


Bei korrekt eingerichteter Firewall ist ein Zugriff vom Klassenzimmernetz ins Verwaltungsnetz und umgekehrt ausgeschlossen.

Auf diese Art herrscht immer noch eine saubere logische Trennung der Netze. Eine physikalische Trennung (die früher einmal gefordert war) ist laut Votum (z.B. Votum 2018 S. 20) schon lange nicht mehr nötig und Routing-Lösungen werden explizit als Möglichkeit genannt.

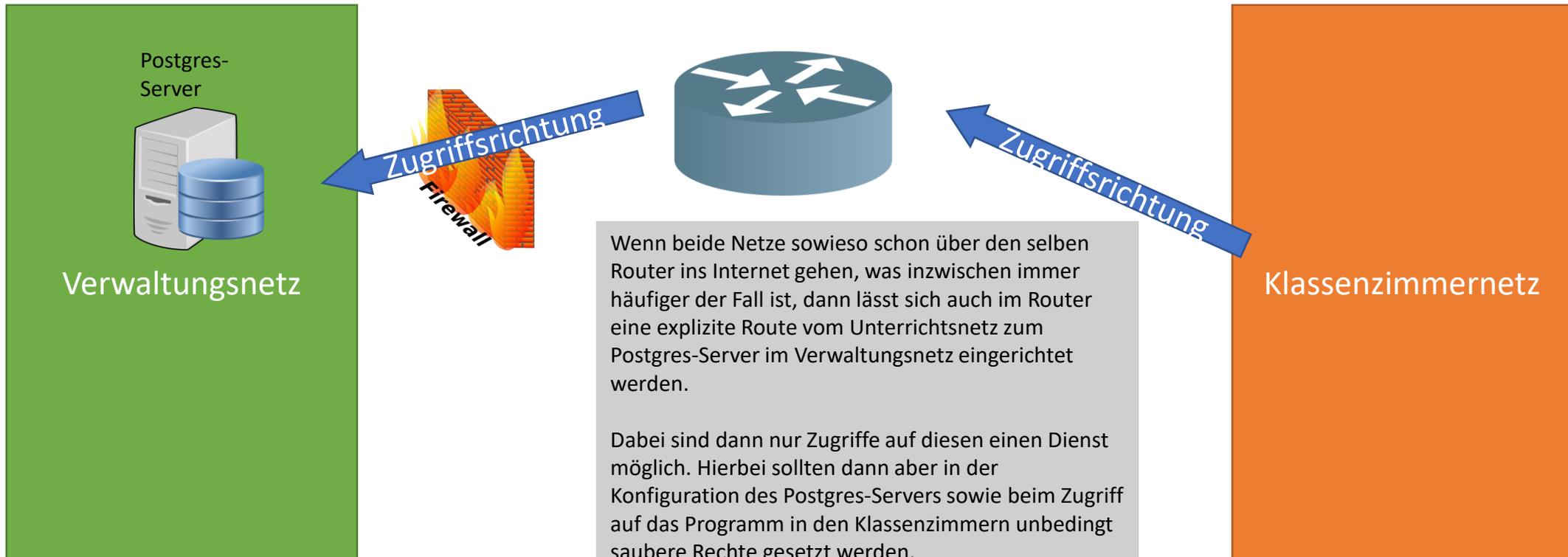
(https://www.mebis.bayern.de/wp-content/uploads/sites/2/2018/06/Votum_2018.pdf)

DMZ-Variante mit WebApp im Klassenzimmer



In diesem Fall ist trotz der Verwendung einer WebApp sogar noch eine zusätzliche Hürde eingebaut, da die Clients aus dem Klassenzimmer und gegebenenfalls WLAN/BYOD-Netz lediglich den internen WebServer in der DMZ erreichen können. Dieser liefert dann nach einem verschlüsselten Login auch lediglich die aktuell anzuzeigenden Daten. Der WebServer kommuniziert dann wiederum als einziger („von rechts aus“) direkt mit dem Postgres-Server. Die SABS2-Hauptanwendung im Verwaltungsnetz kontaktiert den Postgres-Server weiterhin direkt.

Routing-Variante mit Windows-Client im Klassenzimmer



Wenn beide Netze sowieso schon über den selben Router ins Internet gehen, was inzwischen immer häufiger der Fall ist, dann lässt sich auch im Router eine explizite Route vom Unterrichtsnetz zum Postgres-Server im Verwaltungsnetz eingerichtet werden.

Dabei sind dann nur Zugriffe auf diesen einen Dienst möglich. Hierbei sollten dann aber in der Konfiguration des Postgres-Servers sowie beim Zugriff auf das Programm in den Klassenzimmern unbedingt saubere Rechte gesetzt werden.

Es ist auch zu überlegen eine zweite, von ASV und Notenmanager getrennte Postgres-Instanz parallel zu installieren, die über einen anderen Port angesprochen wird, um die potentiellen Zugriffsmöglichkeiten minimal zu halten.

Alles andere ist weiterhin sicher getrennt.

Routing-Variante mit WebApp im Klassenzimmer

