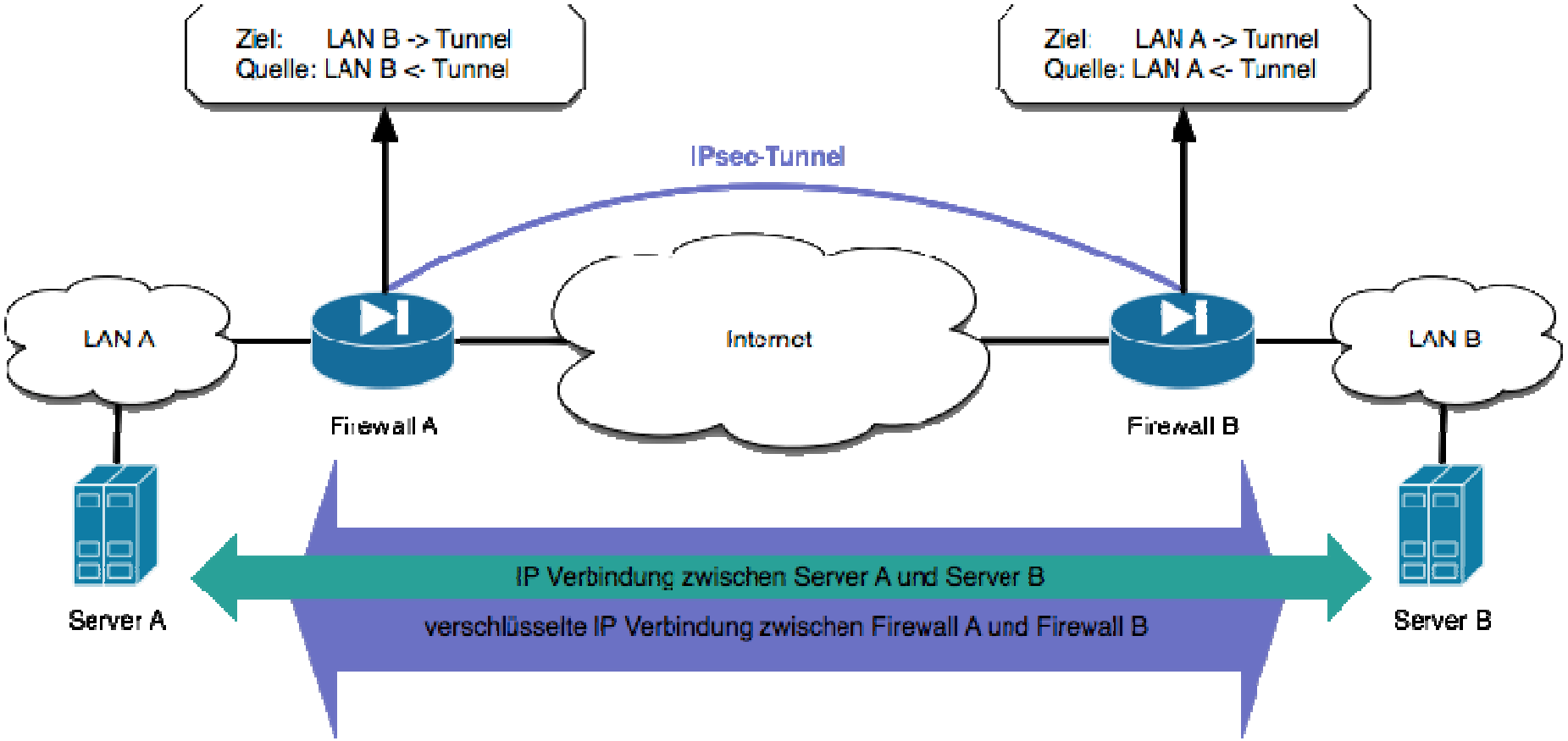
# VPN-Techniken

- IPsec: „klassisches“ VPN
  - z.B. SecuRemote, Cisco IPsec, vpnc, ...
- SSL: „modernes“ VPN
  - z.B. stunnel, openVPN, anyconnect, openconnect, ...

# IPsec

- Setzt auf IP auf
- Meist im Tunnel-Mode benutzt:
  - Nur die Verbindung zwischen den Firewalls wird verschlüsselt
  - Im LAN unverschlüsselt
- Auf beiden Seiten muss die Konfiguration übereinstimmen
- BVB-Firewall kommt mit allen üblichen Konfigurationen zurecht

# IPsec


Ziel: LAN B -> Tunnel
Quelle: LAN B <- Tunnel
Ziel: LAN A -> Tunnel
Quelle: LAN A <- Tunnel
IPsec-Tunnel
LAN A
Internet
LAN B
Firewall A
Firewall B
Server A
Server B
IP Verbindung zwischen Server A und Server B
verschlüsselte IP Verbindung zwischen Firewall A und Firewall B

# Secure Socket Layer (SSL)

- Setzt auf TCP auf
- Verschlüsselung zwischen den Endpunkten
- z.B. HTTPS zwischen Browser und Webserver
- Kann für jedes TCP-Protokoll benutzt werden
- Per stunnel „nachrüstbar“
- Neueste Version als Transport Layer Security (TLS) bekannt

# Vergleich IPsec - SSL/TLS

| | IPsec | SSL/TLS |
|---|---|---|
| Konfigurations-aufwand | an jedem Standort einmal | an jedem Server und Client |
| Komplexität der Konfiguration | hoch | gering |
| Sicherheit | hoch | hoch |
| NAT | problematisch | kein Problem |
| Skalierung | ein Tunnel für alle Dienste | für jeden Dienst extra |