Firewall

Grundlagen

Firewall: Was ist das?

- Aufgaben
  - Trennung mindesten zweier Netzbereiche (WAN/LAN)
  - Kontrollierte Weiterleitung von Paketen
- Anforderungen
  - Verlässlichkeit der Werkzeuge
  - Anpassbare Funktionalität

Was bedeutet dies?

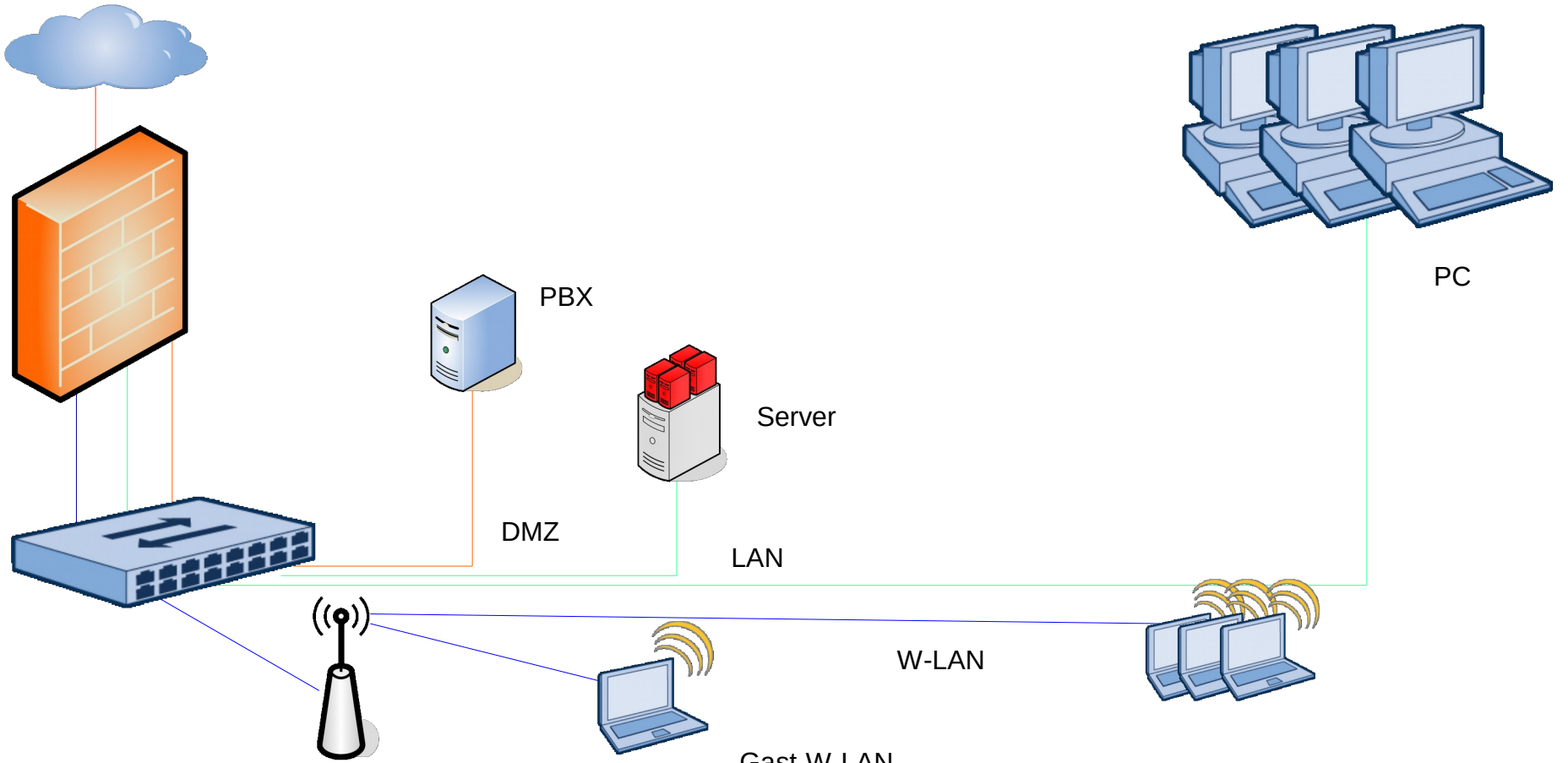
- Quelloffene Werkzeuge
- Verbot von proprietären Lösungen
- Eigene Entscheidung statt Automatik
- Reduzierung auf das Notwendige
- Stabilität
- Anpassbarkeit

Was also?

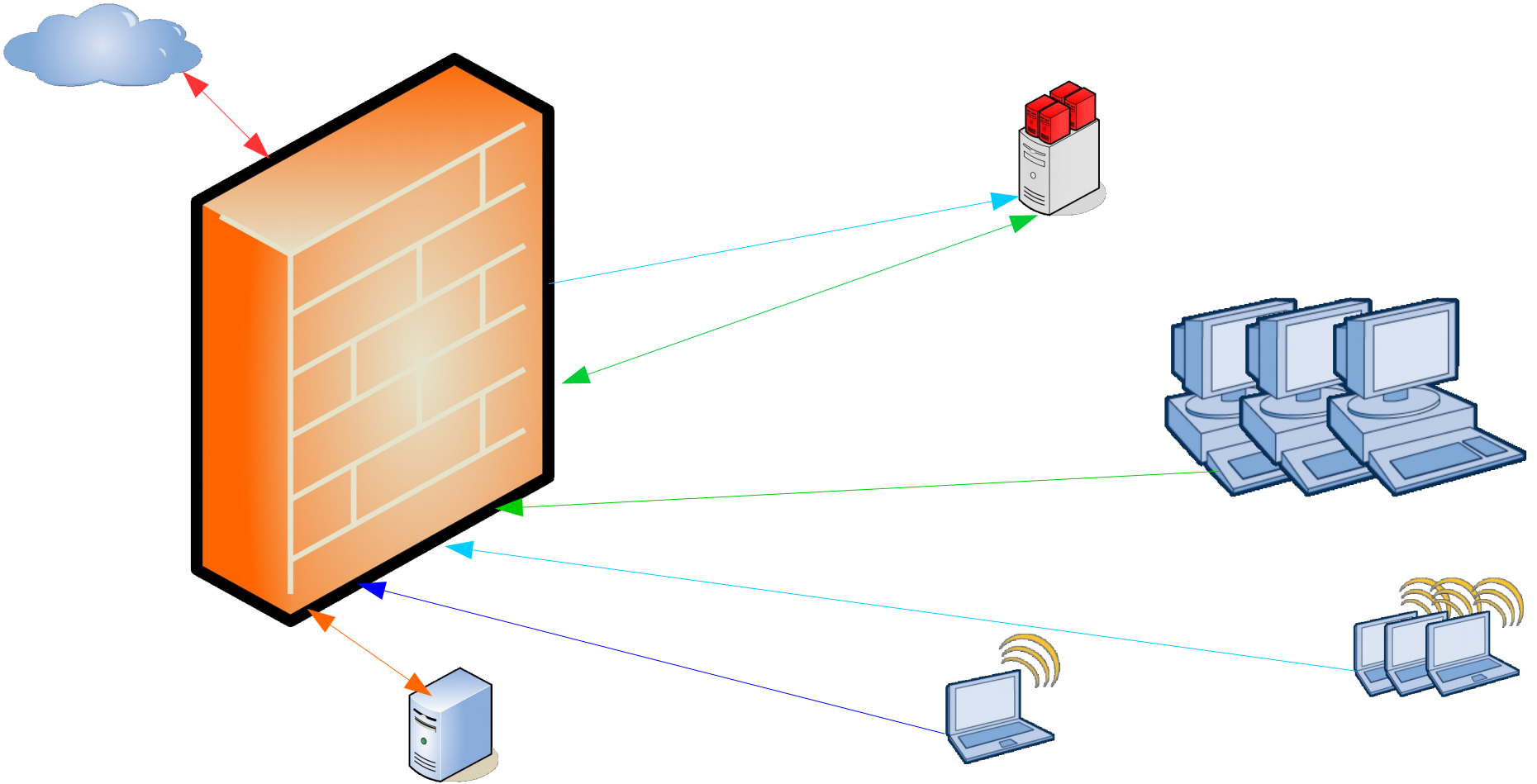
- Iptables (Linux) bzw. Packetfilter (BSD) sind die Basis
- Laufen auf minimalistischem Betriebs-System
- Richten sich an „Wissende“
- Beispiele:
  - IPCop
  - Smoothwall
  - Pfsense
  - Opnsense

Stellung der Firewall im Netzwerk

Das Netzwerk



Netzwerk-Bereiche

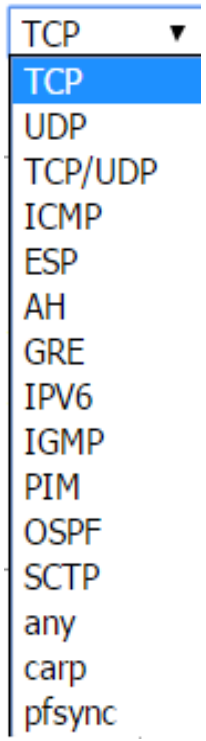


Regel für LAN

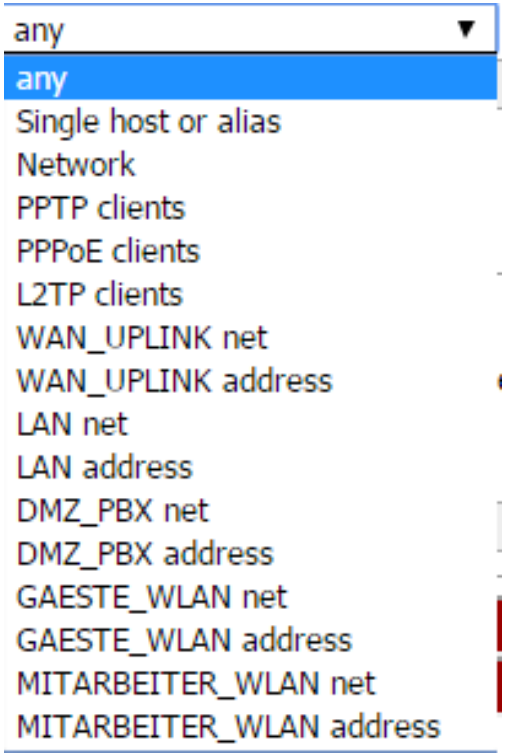
- RDP, TCP inbound, von einer externen IP auf IP des Management-Servers,
  Port 3389, TCP und UDP, maximal eine Verbindung
- SSH, inbound, von einer externen IP auf IP des Daten-Servers,
  Port 22, TCP, maximal eine Verbindung
- SNMP, inbound, outbound, von einer externen IP auf IP des Virtualisier-Hosts
  Port 161, 162, UDP
- Browser/Web
  - HTTP, Port 80 TCP outbound, für alle, nach WAN
  - HTTPS, Port 443 TCP outbound, für alle, nach WAN
- Mail
  - IMAP, StartTLS: Port 143 TCP outbound, für alle, nach WAN
  - SMTP, StartTLS: Port 587 TCP outbound, für alle, nach WAN
- Sonstige Anwendungen
  - HBCI: Port 3000 TCP outbound, begrenzt auf die IP des Buchhaltungs-PC, nach WAN
  - SSH: Port 22 TCP outbound, begrenzt auf die IP des Admins, nach WAN
  - DNS: Port 53 UDP outbound, für alle, nach WAN

Regel-Kriterien

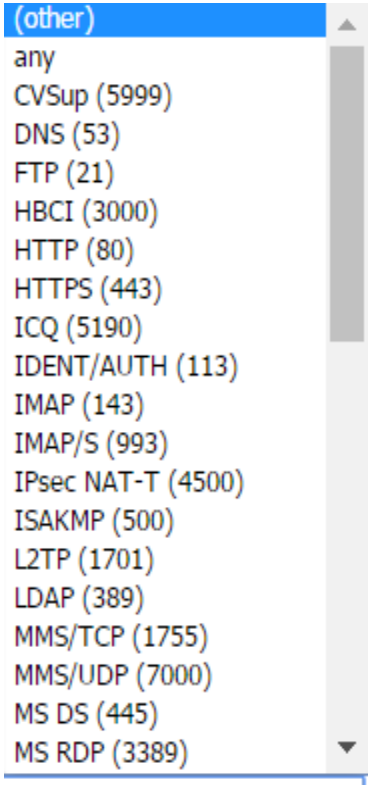
z.B. Protokoll



z.B. Netzwerk-Zone



z.B. Port



Regelwerk

Floating | WAN_UPLINK | LAN | DMZ_PBX | GAESTE_WLAN | MITARBEITER_WLAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
		IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		DNS | Alle
		IPv4 TCP	192.168.115.135	*	*	22 (SSH)	*	none		SSH | Admin
		IPv4 TCP	192.168.115.135	*	*	Mitarbeiter_Ports	*	none		Mitarbeiter-Ports | Admin
		IPv4 TCP	Mitarbeiter	*	*	Mitarbeiter_Ports	*	none		Mitarbeiter_Ports | Mitarbeiter
		IPv4 TCP	192.168.115.125	*	*	3000 (HBCI)	*	none		HBCI | Buchhaltung
		IPv4 TCP	192.168.115.125	*	*	Mitarbeiter_Ports	*	none		Mitarbeiter_Ports| Buchhaltung