

Firewall

Grundlagen

Firewall: Was ist das?

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

Was bedeutet dies?

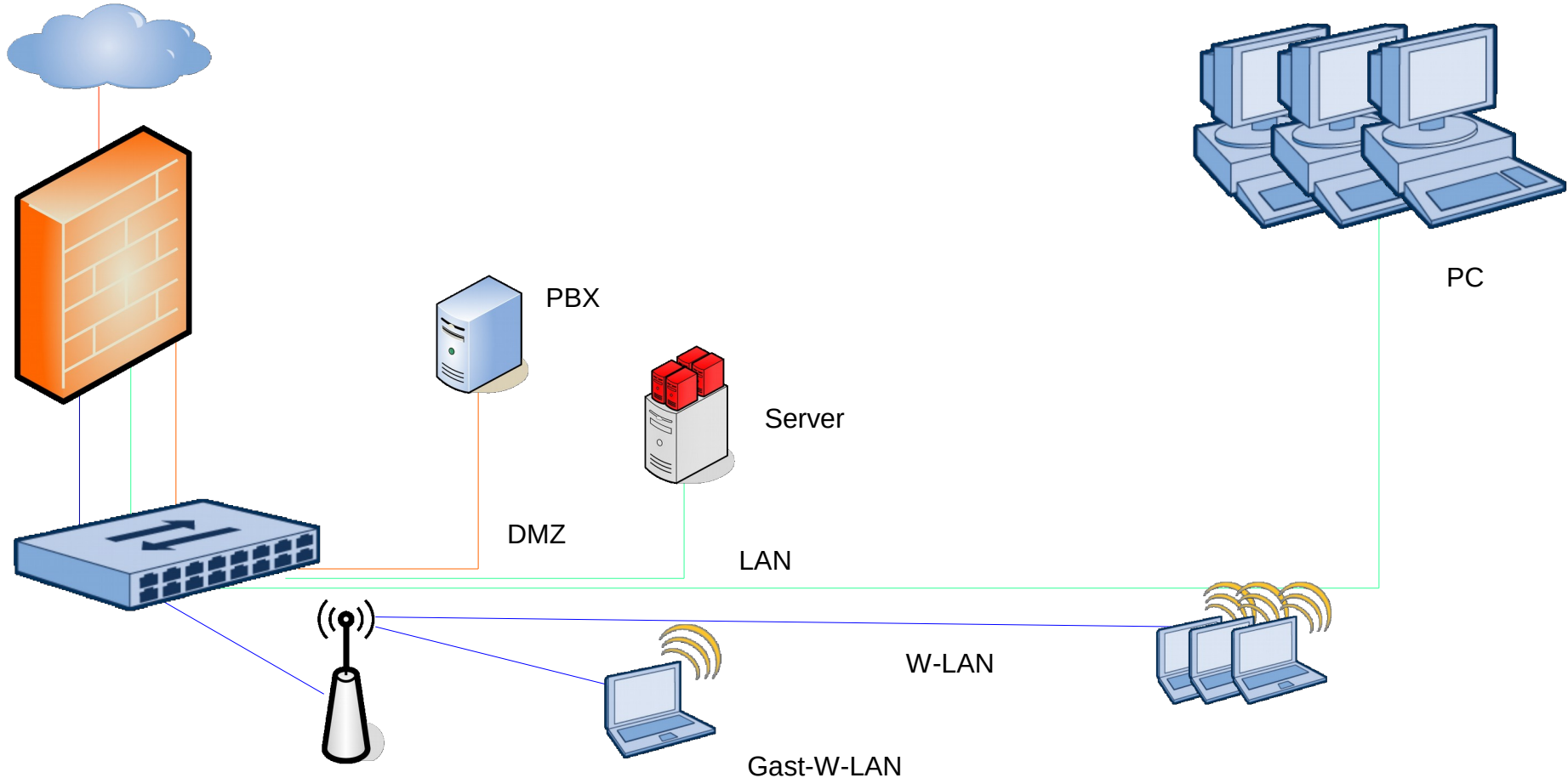
- Quelloffene Werkzeuge
- Verbot von proprietären Lösungen
- Eigene Entscheidung statt Automatik
- Reduzierung auf das Notwendige
- Stabilität
- Anpassbarkeit

Was also?

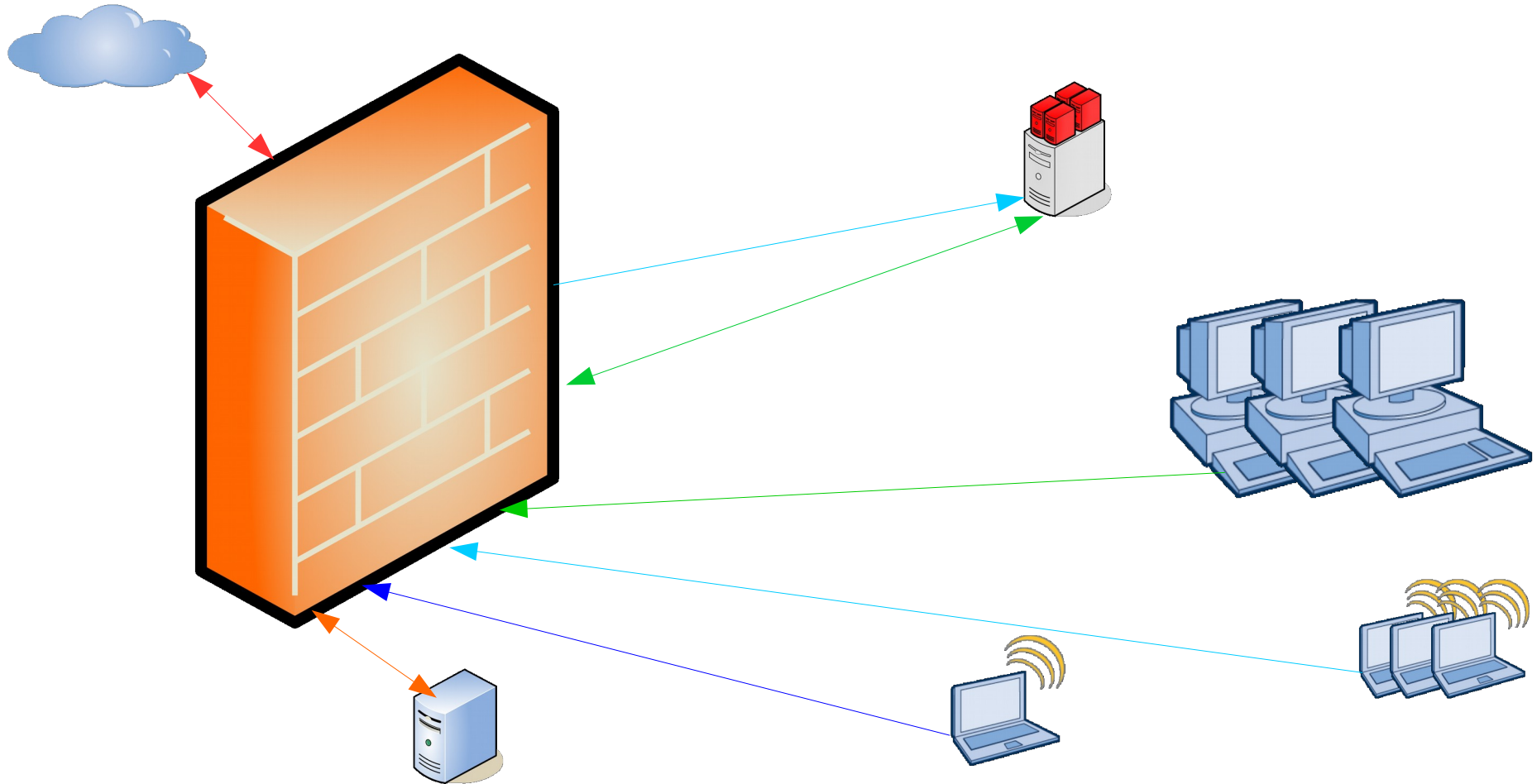
- Iptables (Linux) bzw. Packetfilter (BSD) sind die Basis
- Laufen auf minimalistischem Betriebs-System
- Richten sich an „Wissende“
- Beispiele:
 - IPCop
 - Smoothwall
 - Pfsense
 - Opnsense

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

- TCP
- TCP**
- UDP
- TCP/UDP
- ICMP
- ESP
- AH
- GRE
- IPV6
- IGMP
- PIM
- OSPF
- SCTP
- any
- carp
- pfsync

z.B. Netzwerk-Zone

- any
- any**
- Single host or alias
- Network
- PPTP clients
- PPPoE clients
- L2TP clients
- WAN_UPLINK net
- WAN_UPLINK address
- LAN net
- LAN address
- DMZ_PBX net
- DMZ_PBX address
- GAESTE_WLAN net
- GAESTE_WLAN address
- MITARBEITER_WLAN net
- MITARBEITER_WLAN address

z.B. Port

- (other)**
- any
- CVSup (5999)
- DNS (53)
- FTP (21)
- HBCI (3000)
- HTTP (80)
- HTTPS (443)
- ICQ (5190)
- IDENT/AUTH (113)
- IMAP (143)
- IMAP/S (993)
- IPsec NAT-T (4500)
- ISAKMP (500)
- L2TP (1701)
- LDAP (389)
- MMS/TCP (1755)
- MMS/UDP (7000)
- MS DS (445)
- MS RDP (3389)

Regelwerk

Floating WAN_UPLINK LAN DMZ_PBX GAESTE_WLAN MITARBEITER_WLAN										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		DNS Alle
<input type="checkbox"/>		IPv4 TCP	192.168.115.135	*	*	22 (SSH)	*	none		SSH Admin
<input type="checkbox"/>		IPv4 TCP	192.168.115.135	*	*	<u>Mitarbeiter Ports</u>	*	none		Mitarbeiter-Ports Admin
<input type="checkbox"/>		IPv4 TCP	<u>Mitarbeiter</u>	*	*	<u>Mitarbeiter Ports</u>	*	none		Mitarbeiter_Ports Mitarbeiter
<input type="checkbox"/>		IPv4 TCP	192.168.115.125	*	*	3000 (HBCI)	*	none		HBCI Buchhaltung
<input type="checkbox"/>		IPv4 TCP	192.168.115.125	*	*	<u>Mitarbeiter Ports</u>	*	none		Mitarbeiter_Ports Buchhaltung