

Uwe Stache: Firewalling für KMU

Grundlagen – Szenarien – Best Practices

Gefördert durch:



Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages



Netzwerk Elektronischer
Geschäftsverkehr

Es passt ...



... was zusammen gehört !



Medien

Wirtschaftskompetenz

Bewährte Technik

Neue Gedanken

Definitionen [Firewall]

- Hardware- und regelbasierte Netztrennung
- Drei oder vier Zonen
- Regeln frei definierbar
- Logging

- Zusatzfunktionen:
 - Proxy
 - SPAM-/Virenfilter [in kleinen Netzen]
 - Routerfunktion

Was ist zu schützen?

- Daten
Unternehmensdaten [z. B. Buchhaltung/Kundendaten]
- Ressourcen
eigene Netzanbindung, Rechentechnik, Telefonanlage
- Reputation
Ihre Kunden vertrauen Ihrer Handlungsfähigkeit

Vor wem ist zu schützen?

- Amateure / Spinner
„wollen nur gucken“
- Wettkämpfer / Punktesammler
Punktesystem für Server-Hacks, hinterlassen Logo
- Vandalen
zerstören wahllos
- Spione
verkaufen Ihre Daten
- Interne Dummheit

Schutzmethoden

- Security by Obscurity
Prinzip Hoffnung
- Rechner-zentrierter Schutz
Freigaben- und Ressourcen-Management
- Netzwerk-zentrierter Schutz : **Firewall**

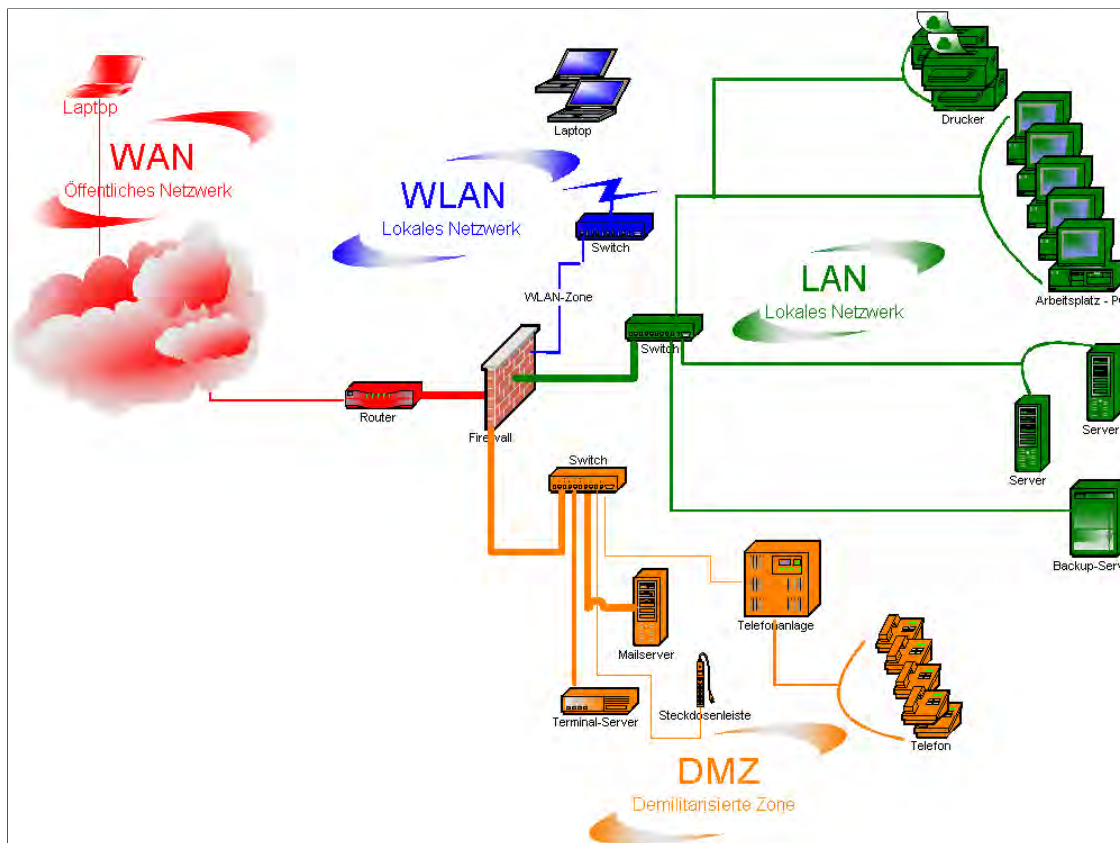
Was bringt eine Firewall?

- Klarheit, Richtlinien, Policy wird erstellt, bevor Firewall gekauft wird
- Zentraler Zugangs-Knoten zum Internet
leichtere Kontrolle
- Dadurch: Begrenzung der Angriffsfläche
- Einen „Single-Point-of-failure“

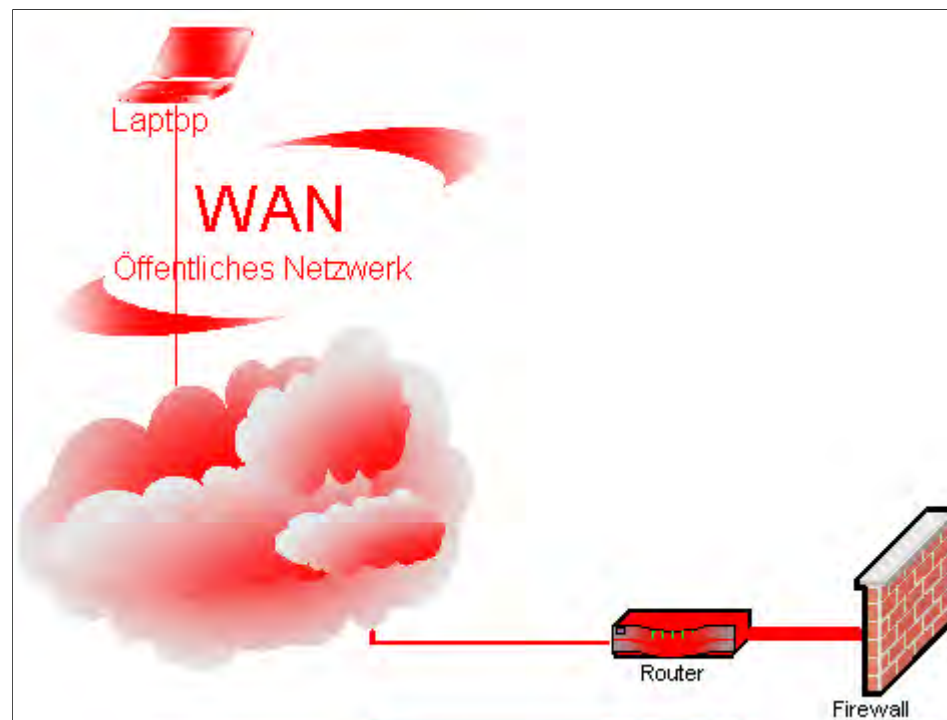
Wovor schützt keine Firewall?

- Angriffe von „Innen“
- Bestandteile von übertragenen Daten
- Angriffe über weitere Netz-Zugänge
z.B. für Fernwartung Telefonanlage
Ersatz-DSL

Netzwerk



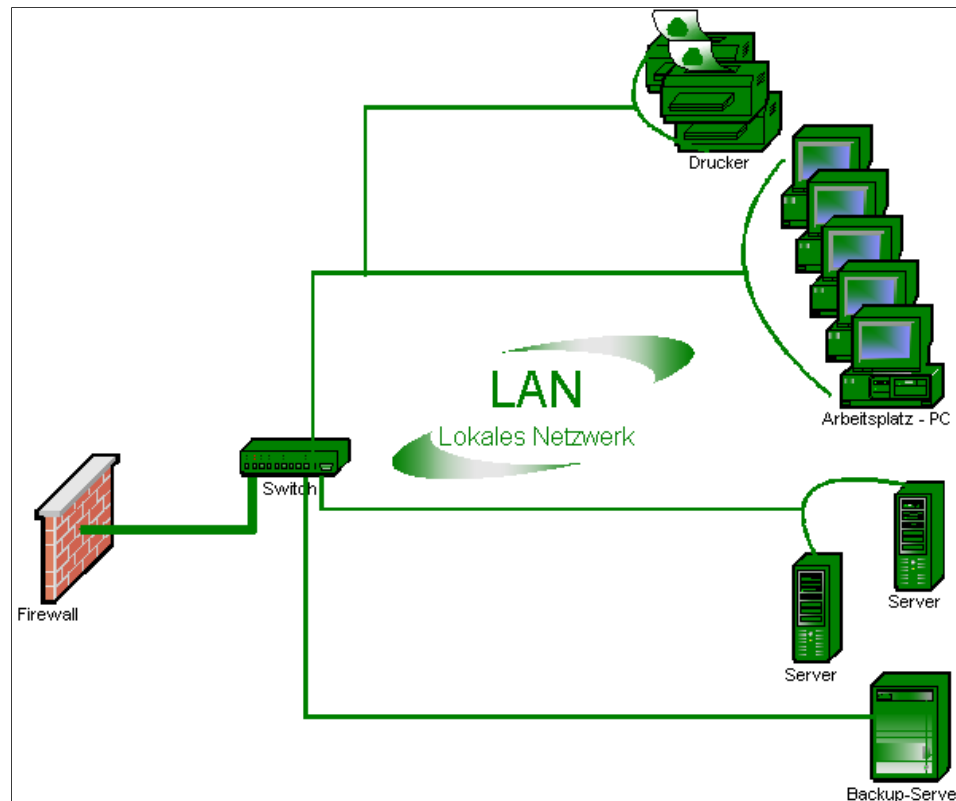
WAN



Definitionen [LAN]

- Lokales Netzwerk
- KEIN Zugriff aus WAN
- Definierte Zugriffe aus DMZ und WLAN
(idealer Weise keine)
- Definierte Zugriffs-Rechte auf andere Zonen

LAN



Regeln

Datenverkehr initiiert von PC:
Ports 80,443,110,25,139,143

Datenverkehr initiiert von
Server:

???

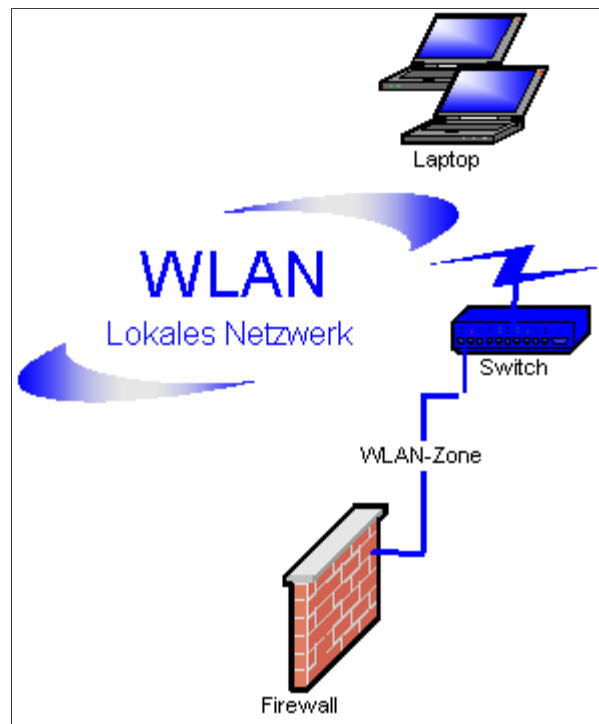
Datenverkehr initiiert von
ausserhalb LAN:

???

Definitionen [WLAN]

- Wireless LAN
- ACL in Firewall via MAC-Adresse
[Access Control List]
- Authentifizierung via WPA-PSK
[minimal]
- Datenverschlüsselung
- Aus WLAN kein Zugriff auf LAN

WLAN



Regeln

Datenverkehr initiiert von Laptop:
25,110,80,143,443

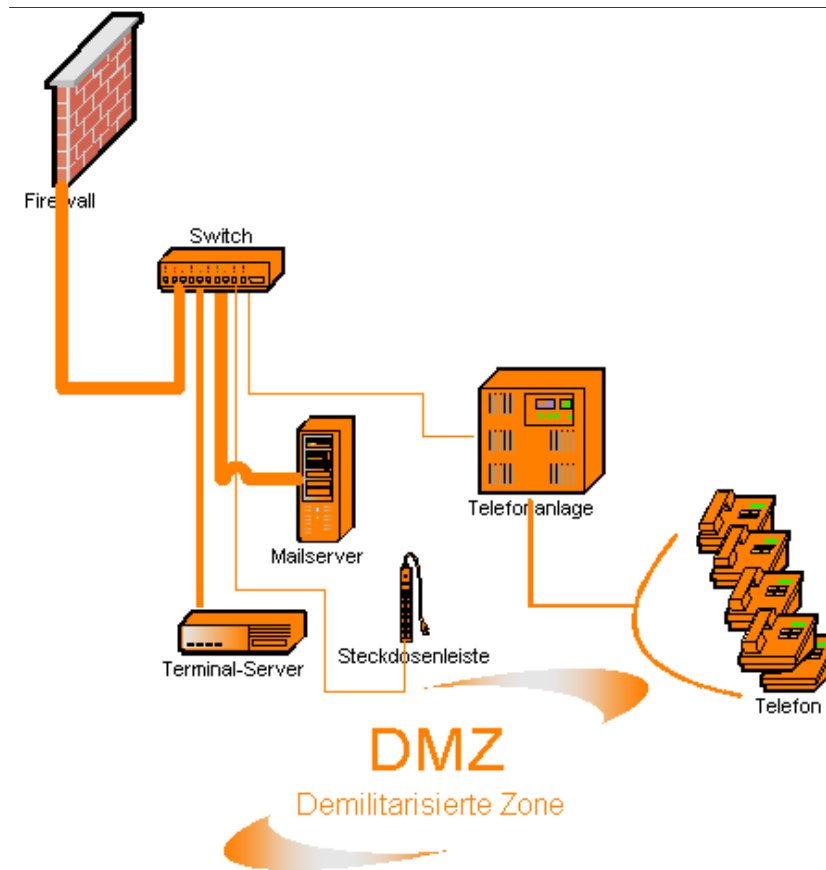
Datenverkehr initiiert von
ausserhalb WLAN:

???

Definitionen [DMZ]

- **Demilitarisierte Zone**
- Ist Teil von WAN **UND** von LAN
- Ist aus WAN definiert erreichbar [z.B. VPN]
- Hat „Schlupflöcher“ zum LAN

DMZ



Regeln

Datenverkehr initiiert von internen Servern:

25,110,143,53

Datenverkehr initiiert von aussen:

25,110,143

Empfehlung / ISO-Distributionen

- IPCOP
schnelle Einrichtung, einfacher Umgang, mehrzonig
- Pfsense
extrem vielseitig, hochlastfähig, mehrzonig, PlugIns
- Weitere:
 - Redwall
 - Smoothwall
 - Sentry
 - Endian
 - ...

Outlook – Versuch einer Perspektive

- IT-Sicherheit heute bereits Kriterium für Basel II
- Paket- und Verbindungs-orientierte Firewall wird ergänzt durch Application Level Firewall
- FW wird „proaktiv“ [?]



Es tut gut,
Wissen zu teilen.

