Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

bwCampusnetz

Einheitliche Sicherheitskontexte und Verwaltung für WLAN und Ethernet

Matthias Machtolf
matthias.machtolf@tik.uni-stuttgart.de
2025-11-25

tik

Was ist ein Sicherheitskontext?

- Sicherheitskontext:
  - **Gruppe** von **IT-Systemen**
  - mit **ähnlichem Schutzbedarf und –Niveau**
  - oft mit **demselben Verantwortlichen**

- Abbildung auf **Netzebene**

- Unabhängig von der **Netzzugangsart**

- Implementierung abhängig von Kontext und Rahmenbedingungen

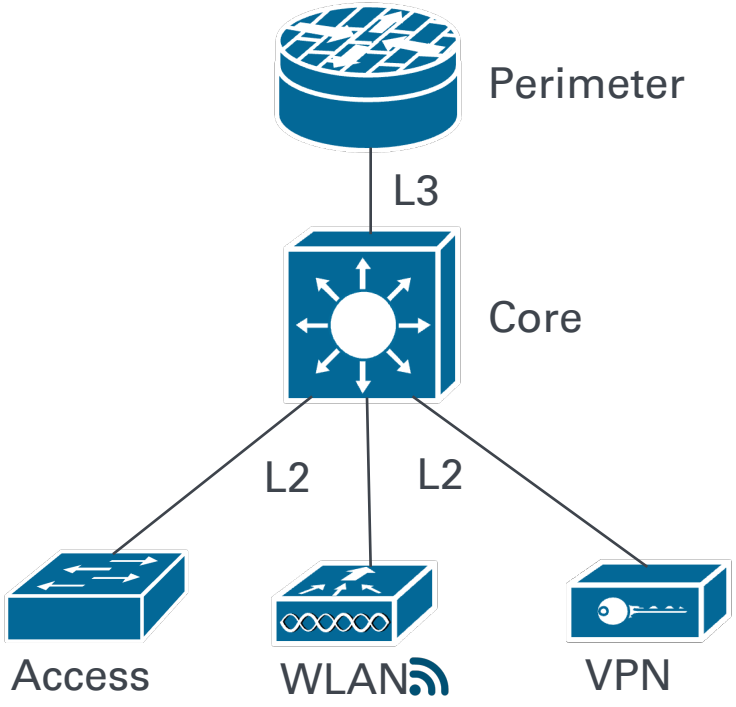
Campusnetze: Bausteine

Netzzugangsarten

- **LAN** (z.B. Statisches VLAN am Access-Port)
- **WLAN** (eduroam Netz(e), Geräte PSK, offenes WLAN)
  → Annahme **Tunnel Mode**
- **VPN**

Campusnetze

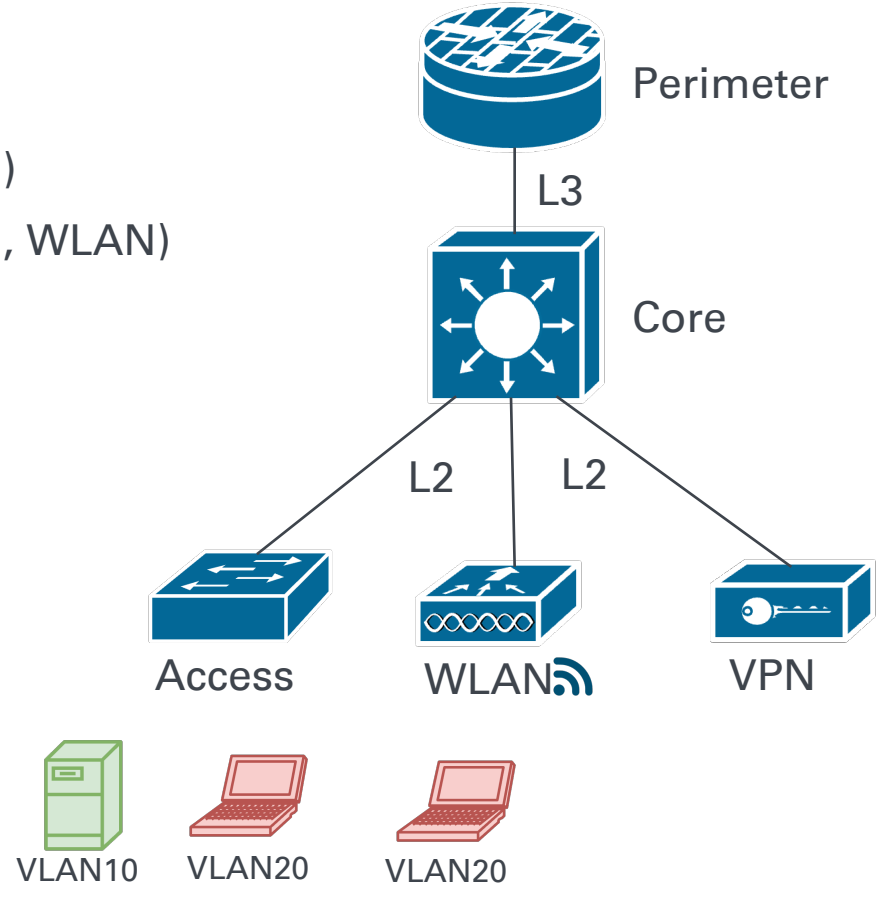
Minimallösung - Collapsed Core



Campusnetze

Minimallösung - Collapsed Core

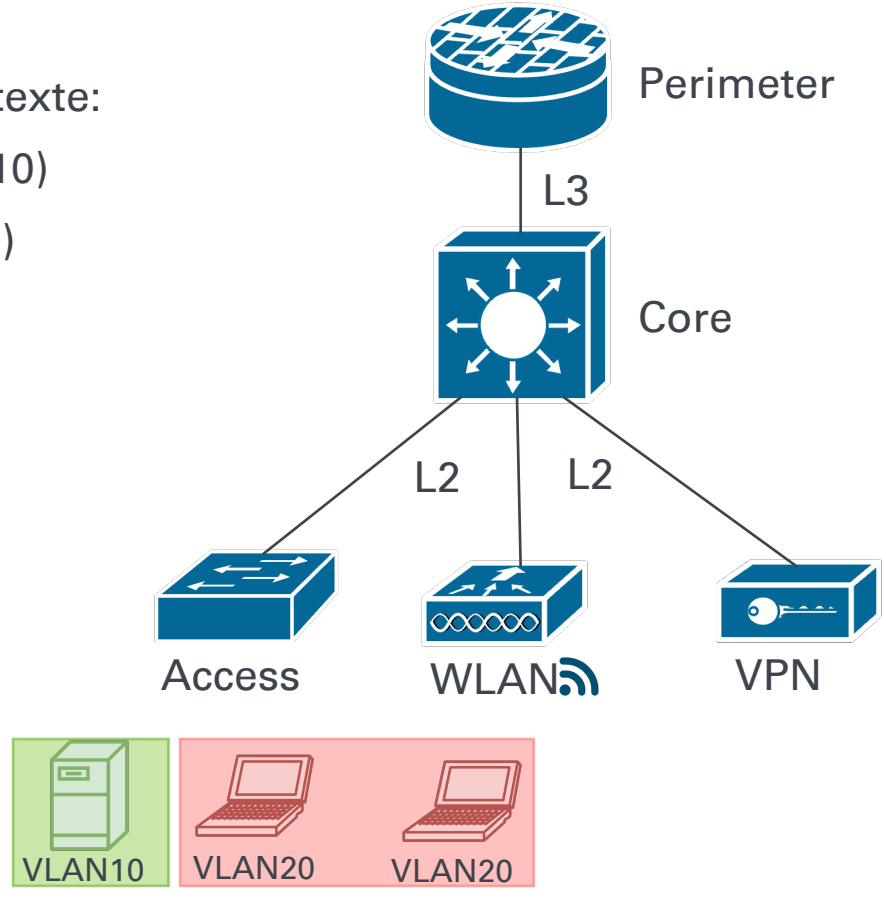
- Präfixe:
  - VLAN10 (LAN)
  - VLAN20 (LAN, WLAN)



Campusnetze

Minimallösung - Collapsed Core

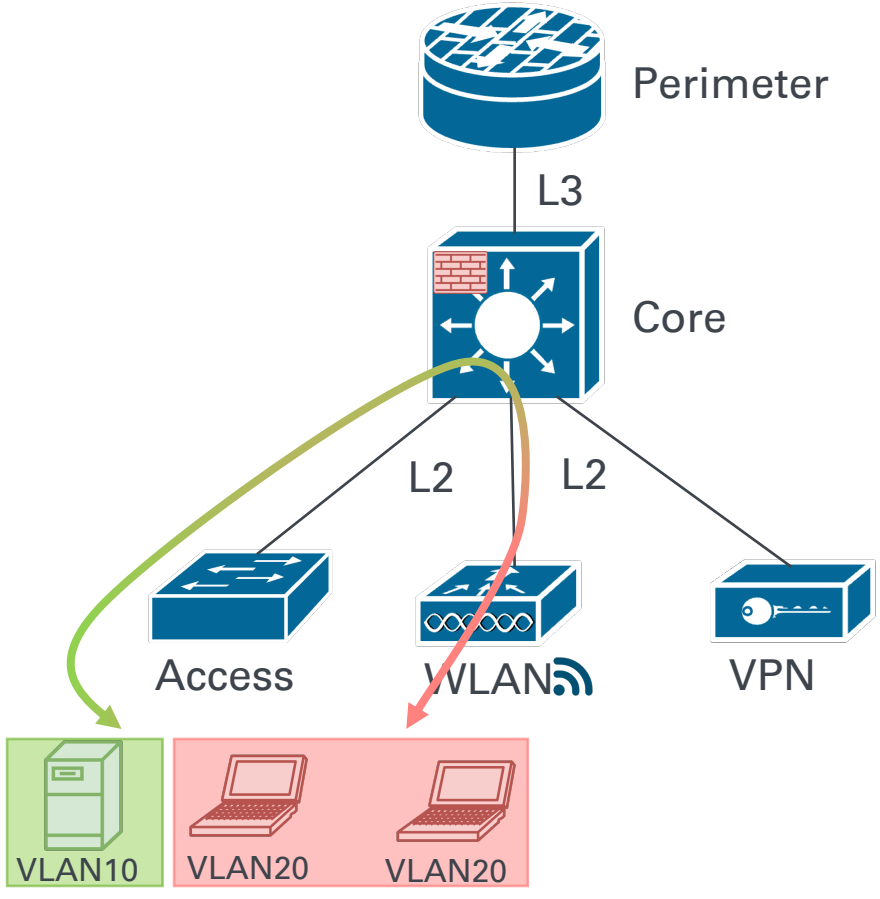
- Sicherheitskontexte:
  - Grün (VLAN 10)
  - Rot (VLAN 20)



Campusnetze

Collapsed Core - (Stateful) Firewall 1

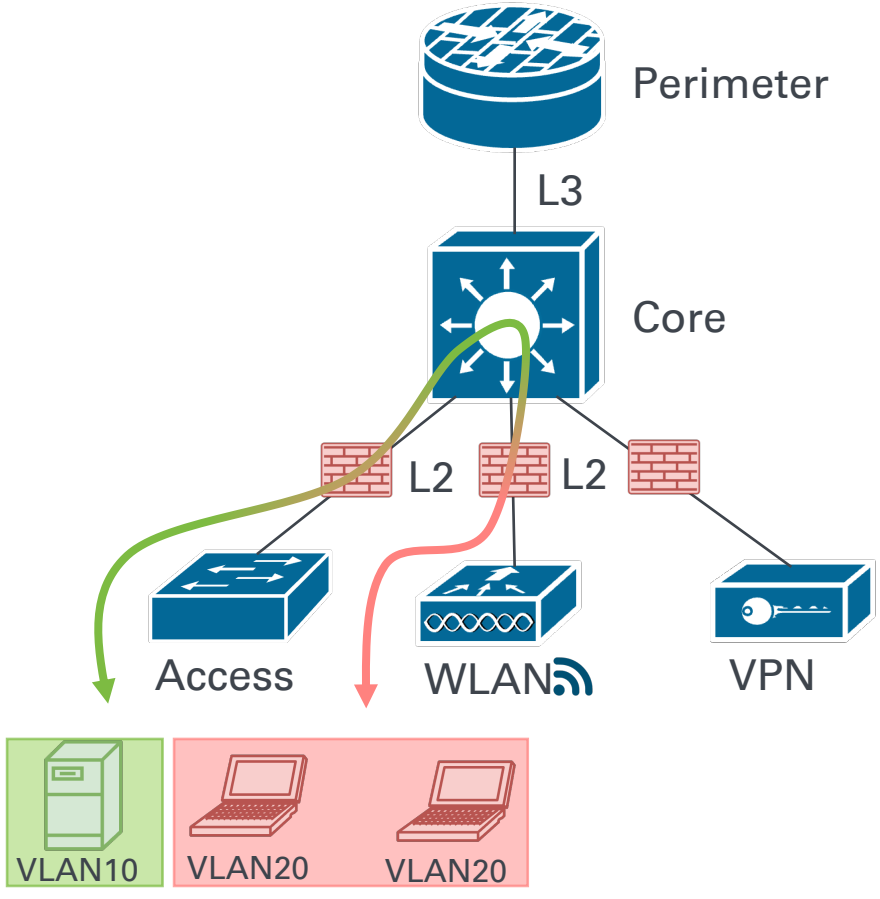
Maßnahme
VLAN
SVI
FW-Gruppe



Campusnetze

Collapsed Core - (Stateful) Firewall 2

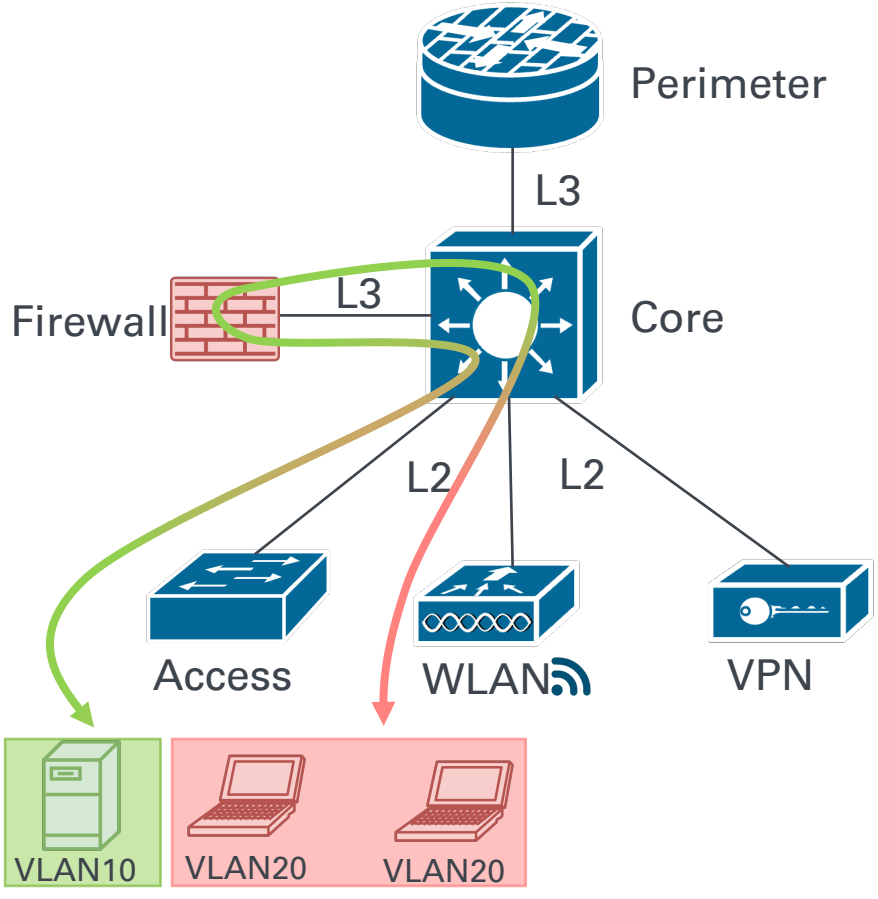
Maßnahme
VLAN
SVI
FW-Gruppe



Campusnetze

Collapsed Core - (Stateful) Firewall 3

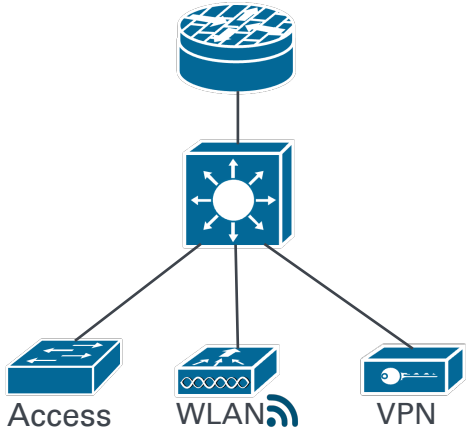
Maßnahme
VLAN
SVI
FW-Gruppe
PBR-ACL



Campusnetze

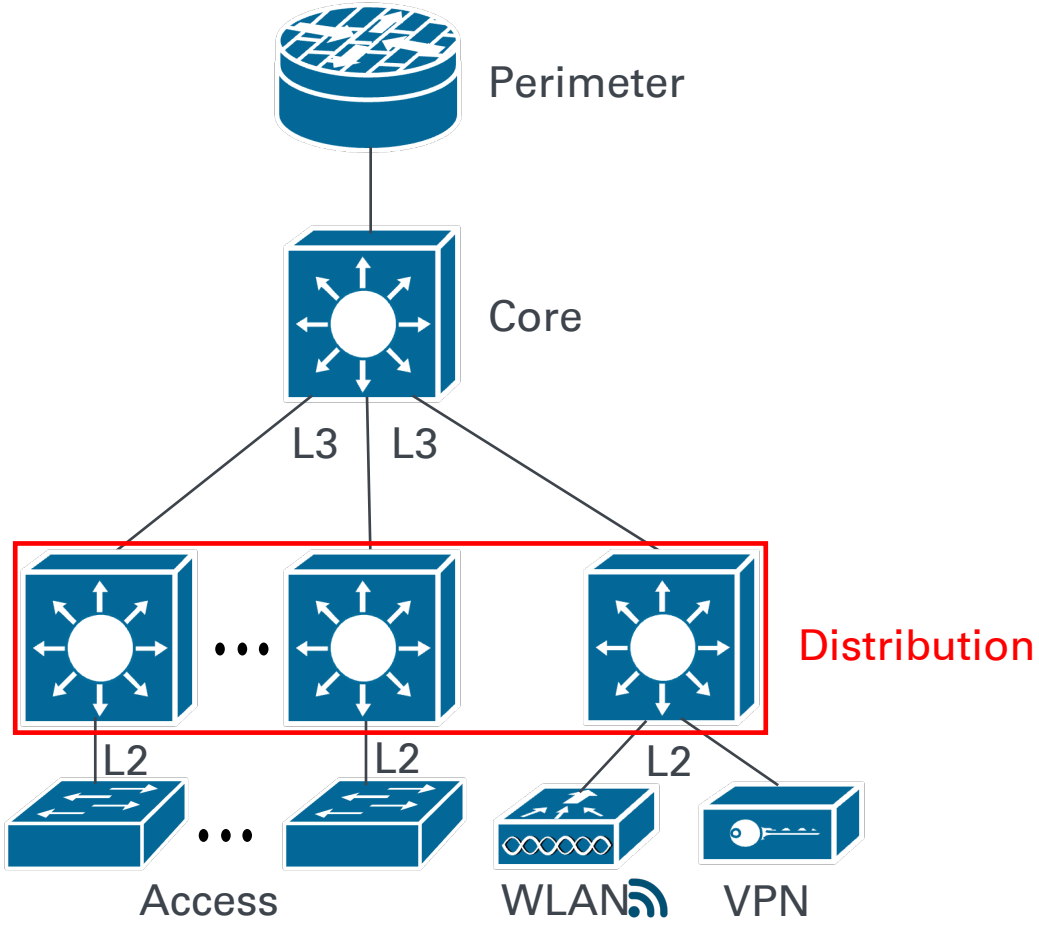
Minimallösung - Collapsed Core

- Anzahl Access-Switche überschaubar
- Kleiner STP-Baum / einfache Topologie
- Begrenzte Skalierungs- und Redundanzanforderungen



Campusnetze: Bausteine

Three-Tier Architecture



Campusnetze

Problem Statement

- VLANs sind **“ortsgebunden“**

- **Layer-3 Trennung** zwischen LAN und WLAN/VPN

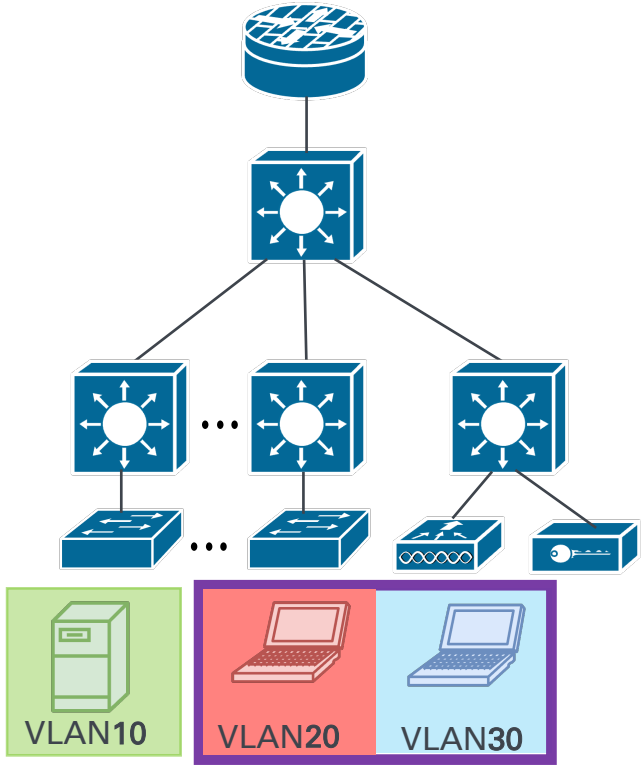
- Access Point als **Bridge** in VLAN
  → Sicherheitsrisiko, Interferenzen

- Separates (Kunden-)VLAN für WLAN/VPN
  → Doppelte Policies, Höherer Betriebsaufwand, (mehr Adressbereiche), ...

Campusnetze

Three-Tier Architecture

- Sicherheitskontext Grün:
  - VLAN 10 (LAN)
- Sicherheitskontext Lila:
  - VLAN 20 (LAN)
  - VLAN 30 (WLAN)

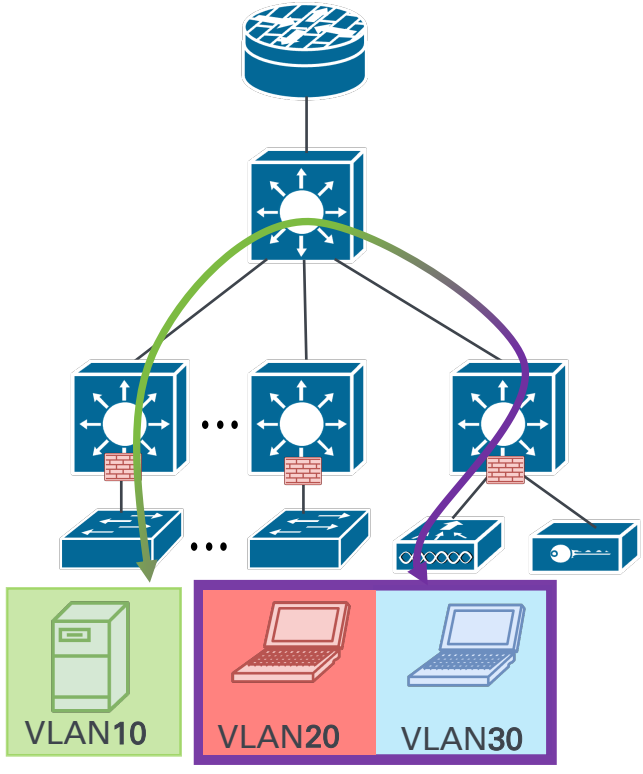


Campusnetze

Three-Tier Architecture - (Stateful) Firewall 1

Maßnahme
VLAN
SVI
FW-Gruppe

- (Stateful) Firewall
  - im Distribution Layer oder
  - zwischen Distribution und Access
- Preis (€€€)
- Management

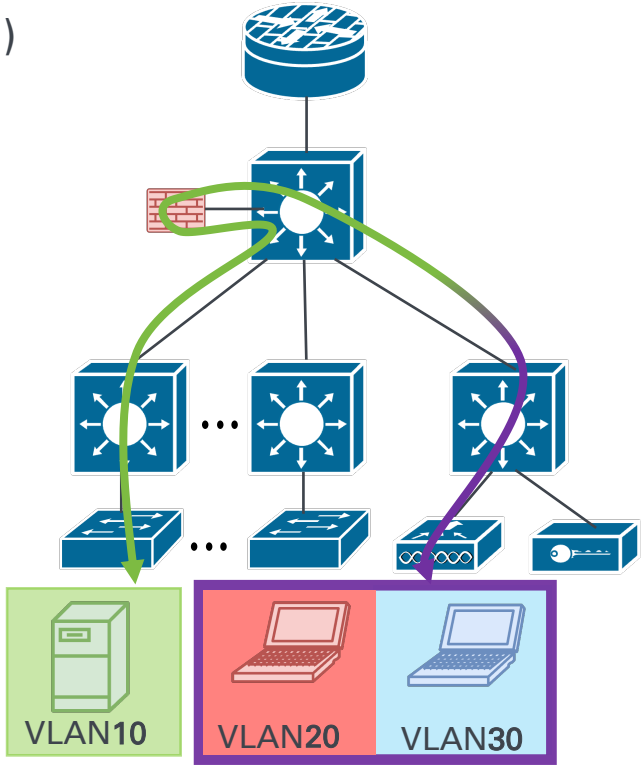


Campusnetze

Three-Tier Architecture - (Stateful) Firewall 2

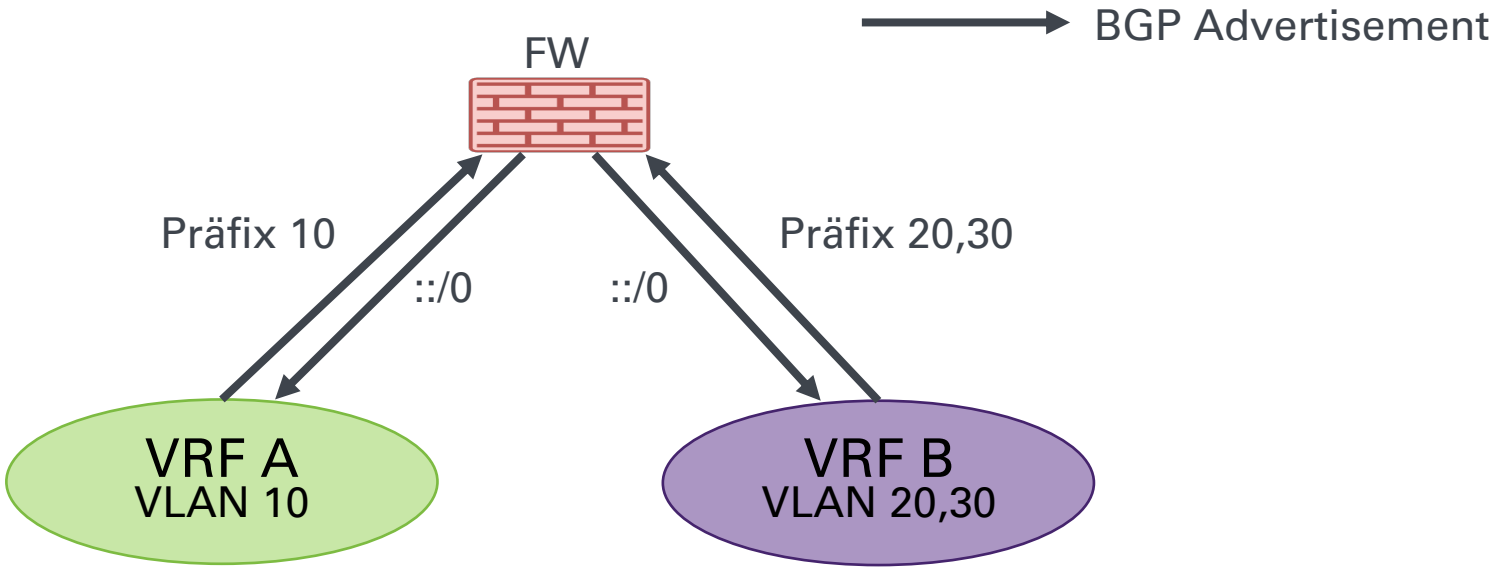
Maßnahme
VLAN
SVI
FW-Gruppe
PBR(-ACL)

- Multi-Hop PBR zur Firewall („On-a-Stick“)
- Skalierbarkeit
- Troubleshooting



Campusnetze

Three-Tier Architecture - (Stateful) Firewall 3



Netzwerkvirtualisierung

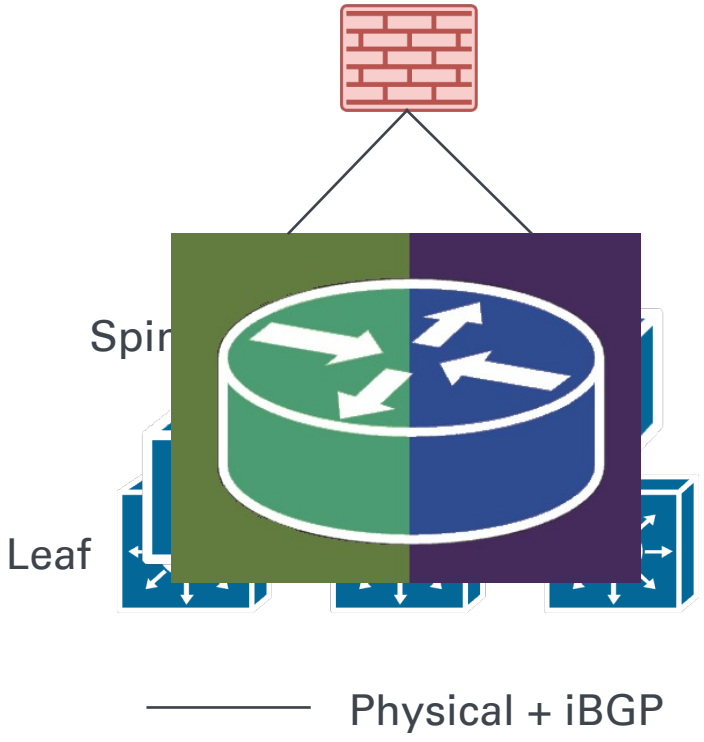
VXLAN + Ethernet VPN

- Data Plane: VXLAN
- Control Plane: Ethernet VPN (EVPN)

- BGP-basierter L2VPN/L3VPN Service

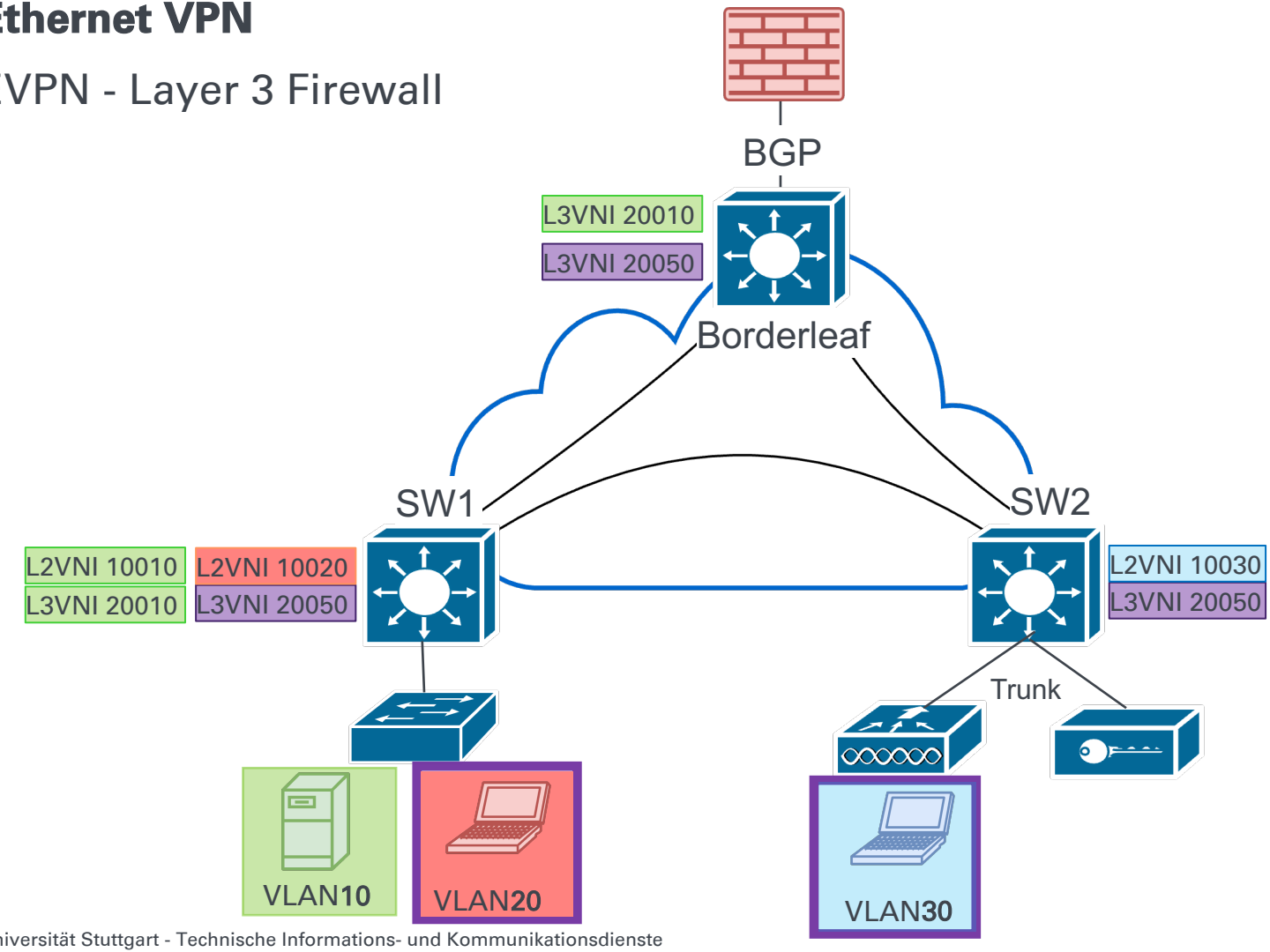
- MAC-VRF:L2VNI = 1:1
- IP-VRF:L3VNI = 1:1

- Alternativ: LISP, Geneve, ...



Ethernet VPN

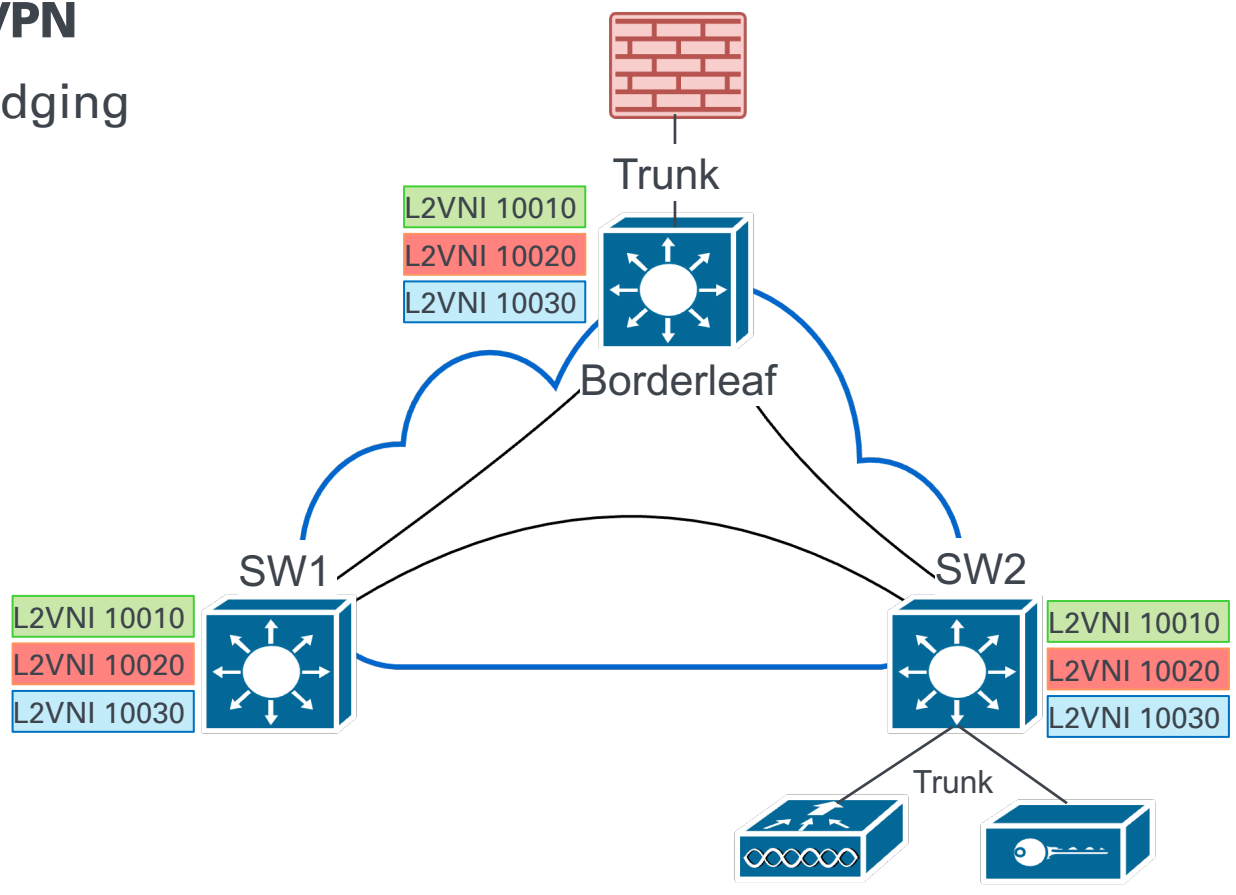
EVPN - Layer 3 Firewall



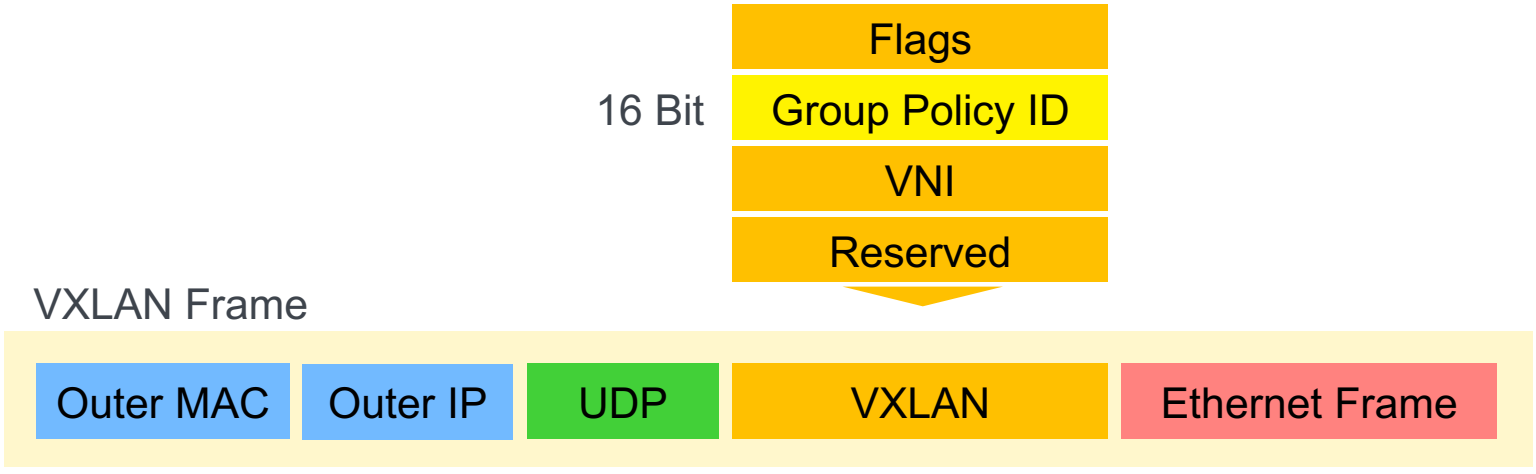
Maßnahme
VLAN
SVI
FW-Gruppe
VRF
VNI
BGP

Ethernet VPN

EVPN - Bridging



VXLAN Group Policy



Fazit

- **Spannungsfeld** aus:
  - Nutzererlebnis
  - Betriebsaufwand und -kompetenz
  - Kosten

- **VLAN-Ansatz** für kleine Netze effizient

- **Overlay** als saubere, flexible Lösung, erfordert Expertise

Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

Vielen Dank!

Matthias Machtolf

E-Mail matthias.machtolf@tik.uni-stuttgart.de
Telefon +49 (0) 711 685-87301
www.tik.uni-stuttgart.de

Universität Stuttgart
Technische Informations- und Kommunikationsdienste (TIK)
Allmandring 30A
70550 Stuttgart

Campusnetze

Three-Tier Architecture - (Stateful) Firewalling 4