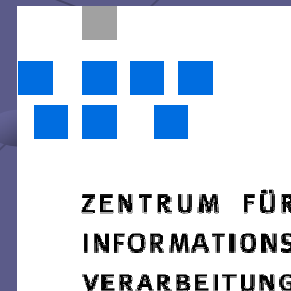


Was bedeutet eigentlich *Strukturierung?*

ZIV-Weiterbildung

Münster 19.1.2007

Georg Richter
Abteilung Kommunikationssysteme im ZIV
richter@uni-muenster.de



Integrierte Sicherheit in Strukturierten Netzen

Virtualisierung
von
Netzstrukturen und Sicherheitselementen
in
Lokalen Rechnernetzen

- ***Grundlagen***
- ***Implementierung***
- ***Strukturen***
- ***Organisation***



Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

● **Vorrang der Endsystem-Sicherheitsmaßnahmen**

- skalierend
- nutzernah – anwendungsbezogen

- Virus Scan
- Personal Firewall
- Update Service
- Host Intrusion Prevention
- Policy Orchestrierung

● **Ergänzung Netzbasierte Sicherheitsmaßnahmen:**

- Infrastrukturbestandteil - elementar, „nicht umgehbar“

- Zugangskontrolle – was oder wer von wo wohin?
 - VLANs, VPNs
 - stateless/stateful packet screening via Access control lists
 - port/tunnel based authentication – IEEE 802.1x, WPA, IPsec VPN
- Intrusion Prevention (Signatur- und verhaltensbasierte Steuerung)
- Verschlüsselung IPSEC, WPA
- NAC/NAP – Security Compliance Enforcement

● **Gateways und Proxies: Anwendungsbezogene Kommunikationssteuerung**

- Inhaltsfilterung: Viren, Spam, URLs – SMTP, FTP, HTTP(S), ...
- Terminalserver als ultimative Steuerungsmöglichkeit
- ...

Details später lesen !

Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

● **Natürliche Aufgabenteilung**

- Systemadministration:
Sicherheit in End- und Anwendungssystemen
End-to-End
- Netzadministration:
Sicherheit im Übermittlungssystem (L1-L3/L4)

Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

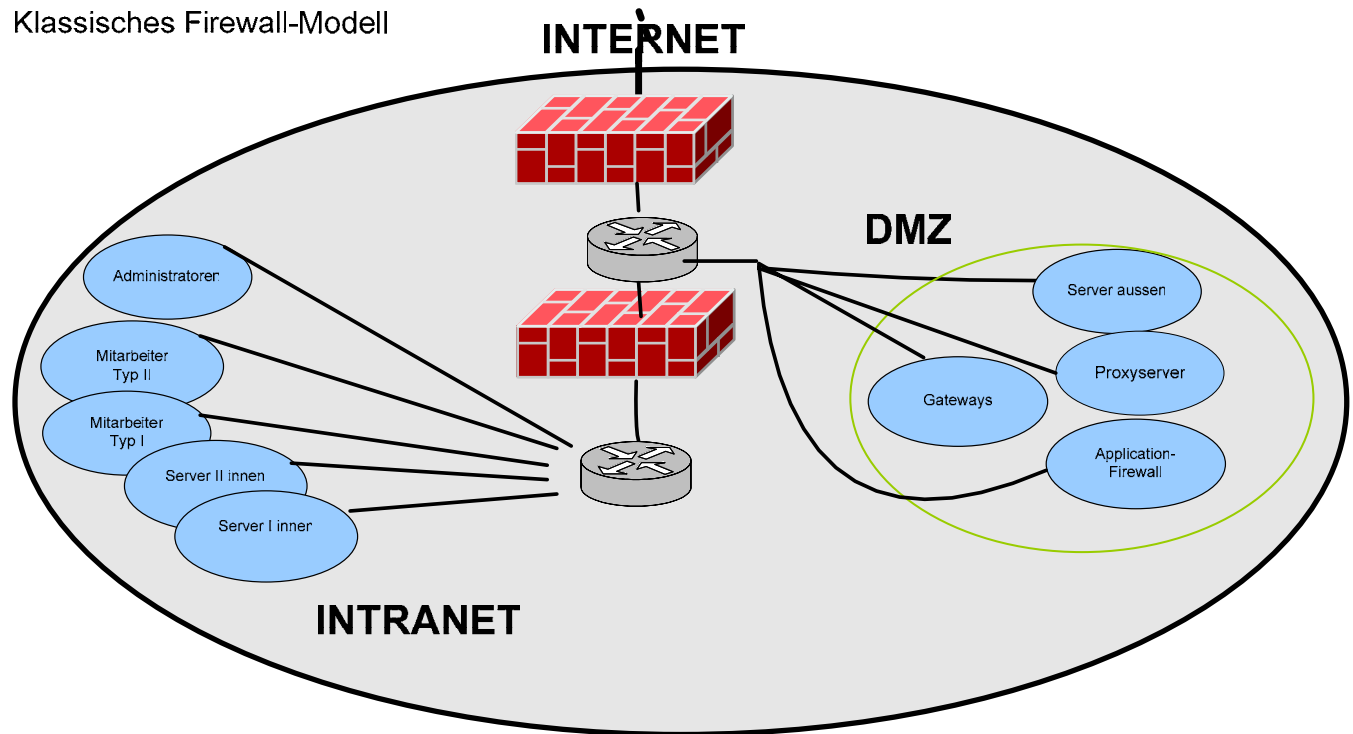
● Sicherheitsmodell Internet/DMZ/Intranet ?






- Unzulänglich für große komplexe Netze
- Probleme bei Vielzahl konventioneller Firewalls im Netz



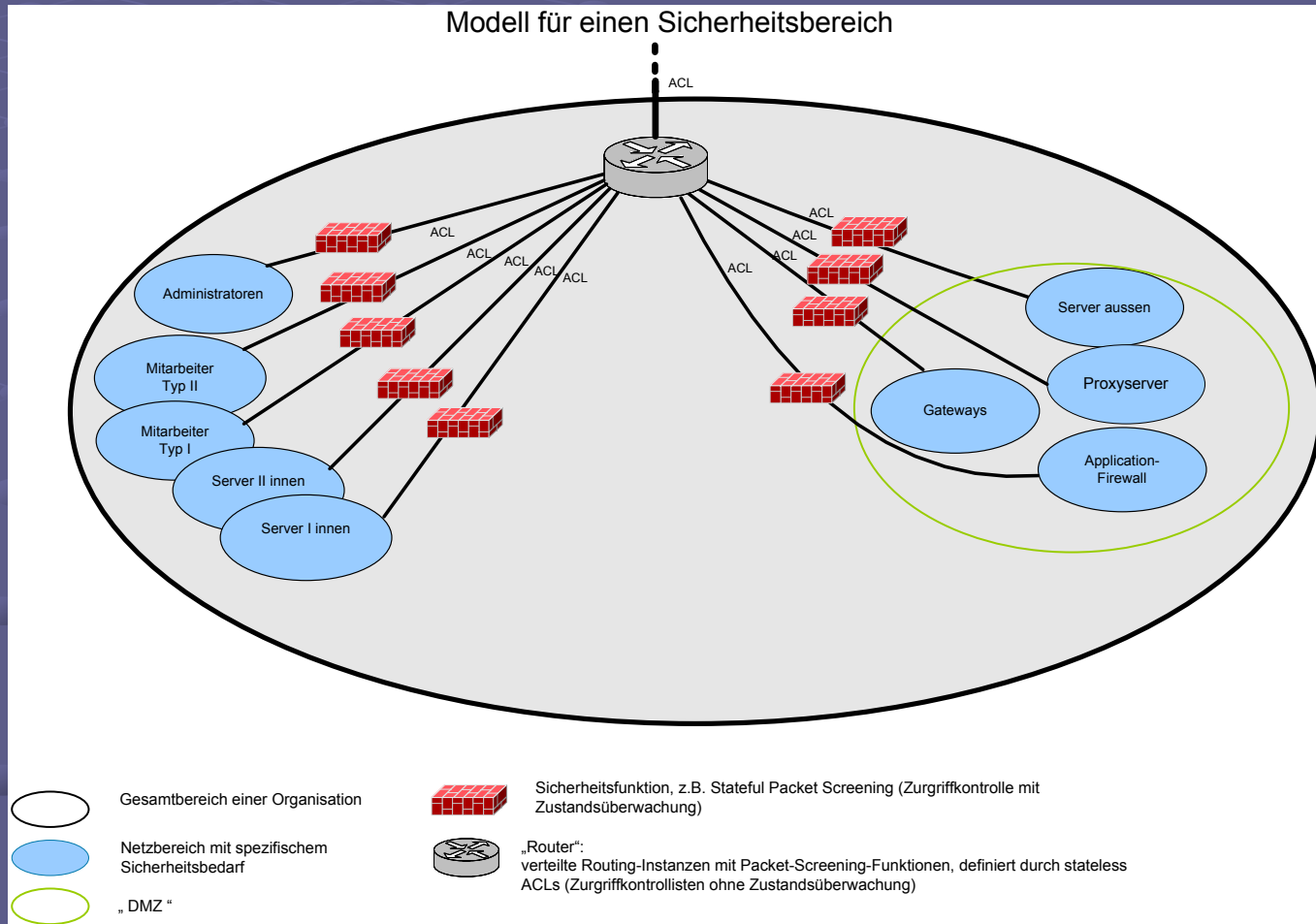
Klassisches Firewall-Modell

Klassisches Firewall-Modell



-  Gesamter Sicherheitsbereich für eine Gruppe von Netzbereichen
-  Netzbereich mit spezifischem Sicherheitsbedarf
-  „DMZ“
-  „Packet Screen“: Stateful Packet Screening (Zugriffskontrolle mit Zustandsüberwachung)
-  „Router“

Strukturieren und schützen im Netz



Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

- **Strukturieren:**
Kommunikationsbereiche einheitlichen Schutzbedürfnisses und gegenseitigen Vertrauens bilden und gegeneinander sichern
 1. Netzzonen/-strukturen (VLANs, Subnetze) bilden, in denen weitgehend ungehindert oder nach einheitlicher Policy einer Nutzergemeinschaft kommuniziert werden darf
 2. Anwendungen, Dienste, Daten, Nutzer und Administratoren auf Endsysteme (Server, Arbeitsplätze) verteilen
 3. Endsysteme den Netzzonen zuordnen
 4. Kommunikation zwischen den Netzzonen sichern (einschränken, Inhalte ggf. filtern) durch netzseitige Einbettung von Systemen mit adäquater Funktion, Leistungsfähigkeit und Parametrierung an geeigneten Stellen im Netz
- Ergebnisoptimierung nach allen Variablen in 1 - 4

Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

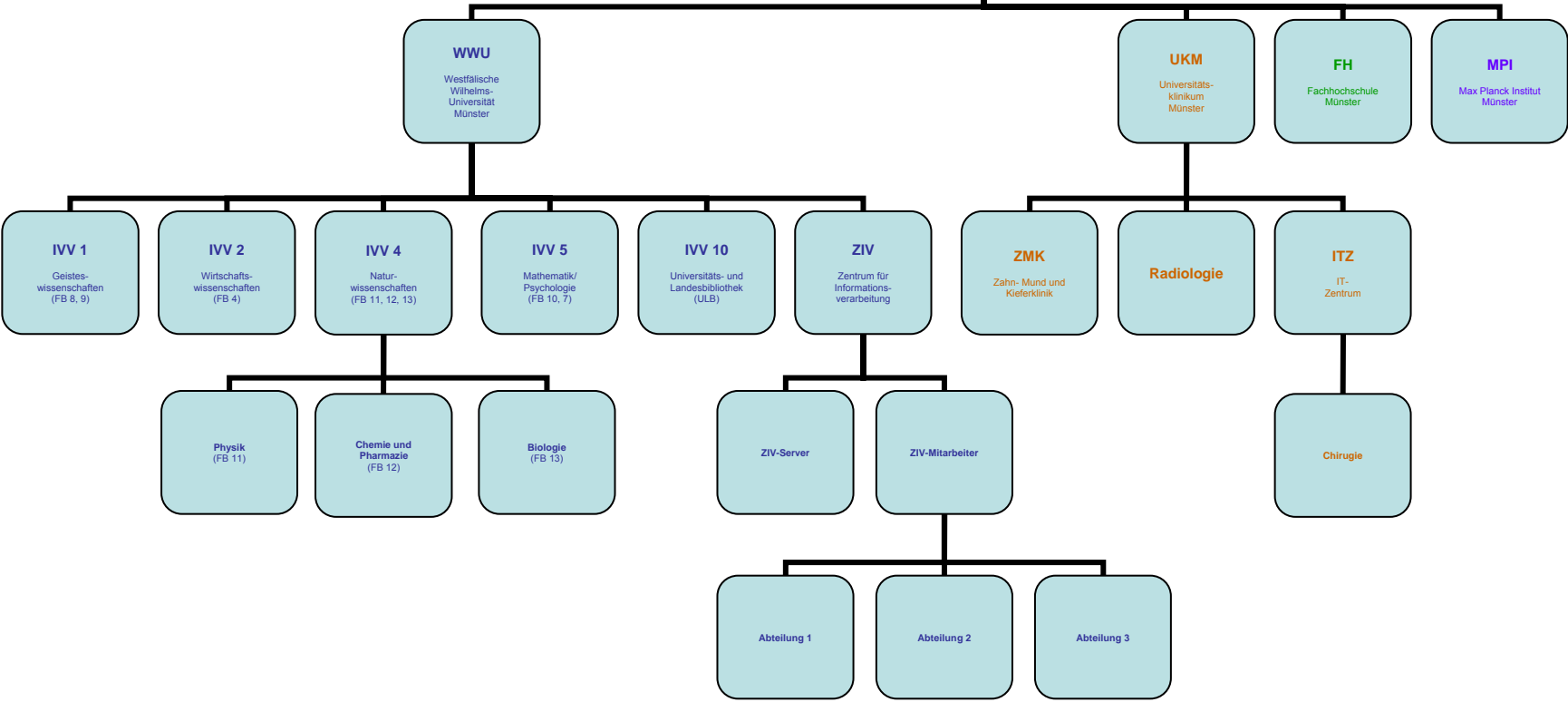
● Hierarchisch strukturieren:

- Sicherung von N Bereichen:
Regelzahl für Kommunikationssteuerung in der Größenordnung N^2
- **Hierarchisierung**
 - Verteilter Ansatz: lokal n^2 Regeln, $\sum n^2 \ll N^2$
 - Adäquate Zuständigkeiten durch Entsprechung in der IT-Organisationshierarchie
- **Optimierung von Kosten und Leistung**
 - Allgemein Nutzung von Standard-Mechanismen und –Technologie möglich
 - ACLs / Stateless Packet Screening in L3-Switches
 - An strategischen Punkten ergänzend zusätzliche Funktionen in das Netz „einbetten“:
 - Stateful Packet Screening
 - IPS
 - VPN

● Klassischer Firewall-Ansatz?

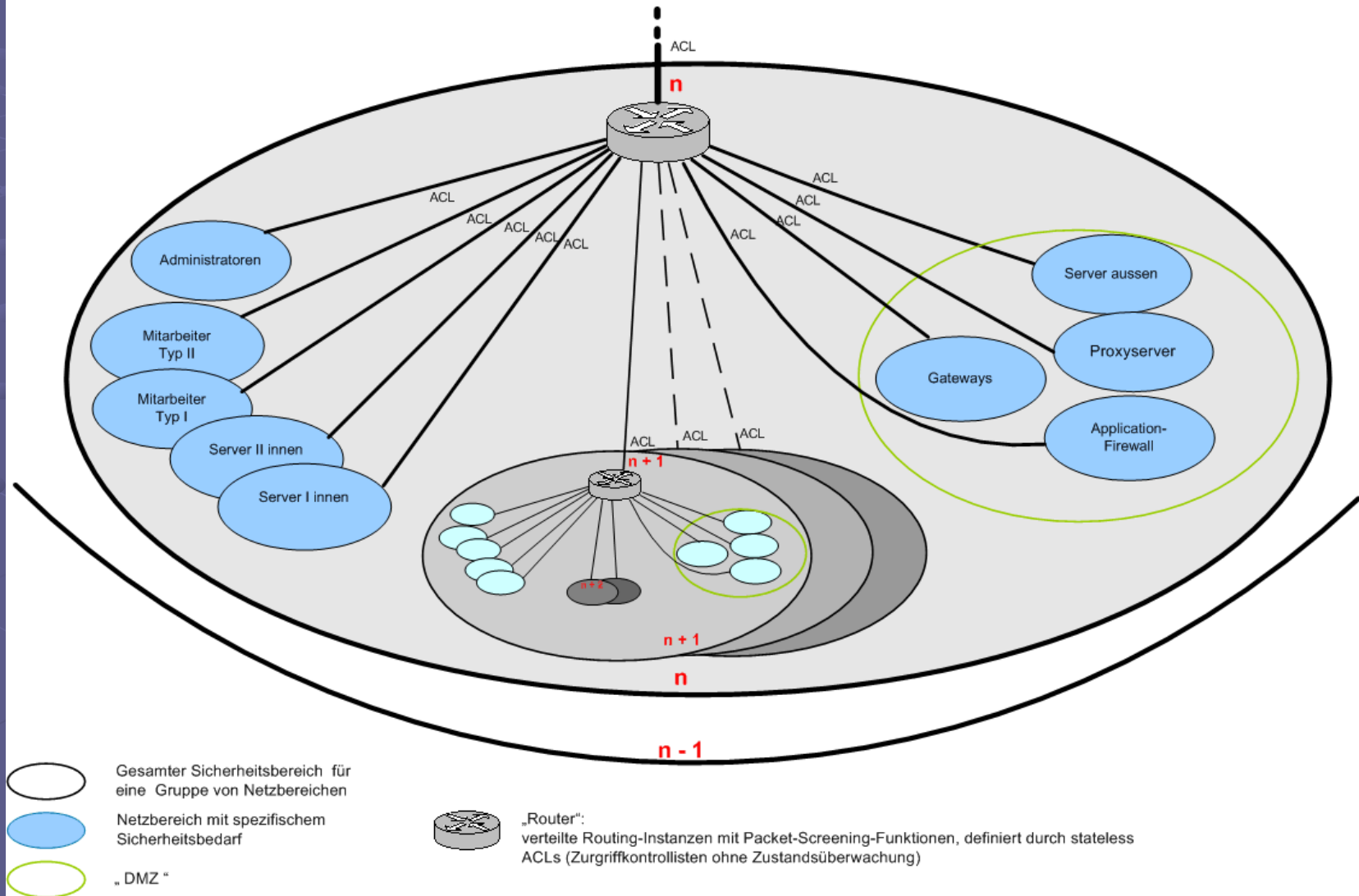
- Monolithischer Ansatz „Firewall“ – Kosten und Leistung
- Verteilter Ansatz – Komplexität

Hierarchische IT-Organisation



Hierarchisch strukturieren und schützen im Netz

Modell für einen Sicherheitsbereich der Stufe n



Wie kann man in großen komplexen Netzen durch netzseitige Maßnahmen die IV-Sicherheit verbessern ?

● Persönlicher VPN-Zugang (*Client-to-Site*)

- Nach „Irgendwo“ - in einzelne Kommunikationsbereiche und in verschiedene Hierarchiezweige
- Von „Irgendwo“, auch aus dem „LAN“
- mit differenzierter Autorisierung nach Ziel bzw. Nutzergruppenzugehörigkeit:
karl.maier@admin.mathe.uni-muenster.de

● Site-to-Site-VPN-Zugang

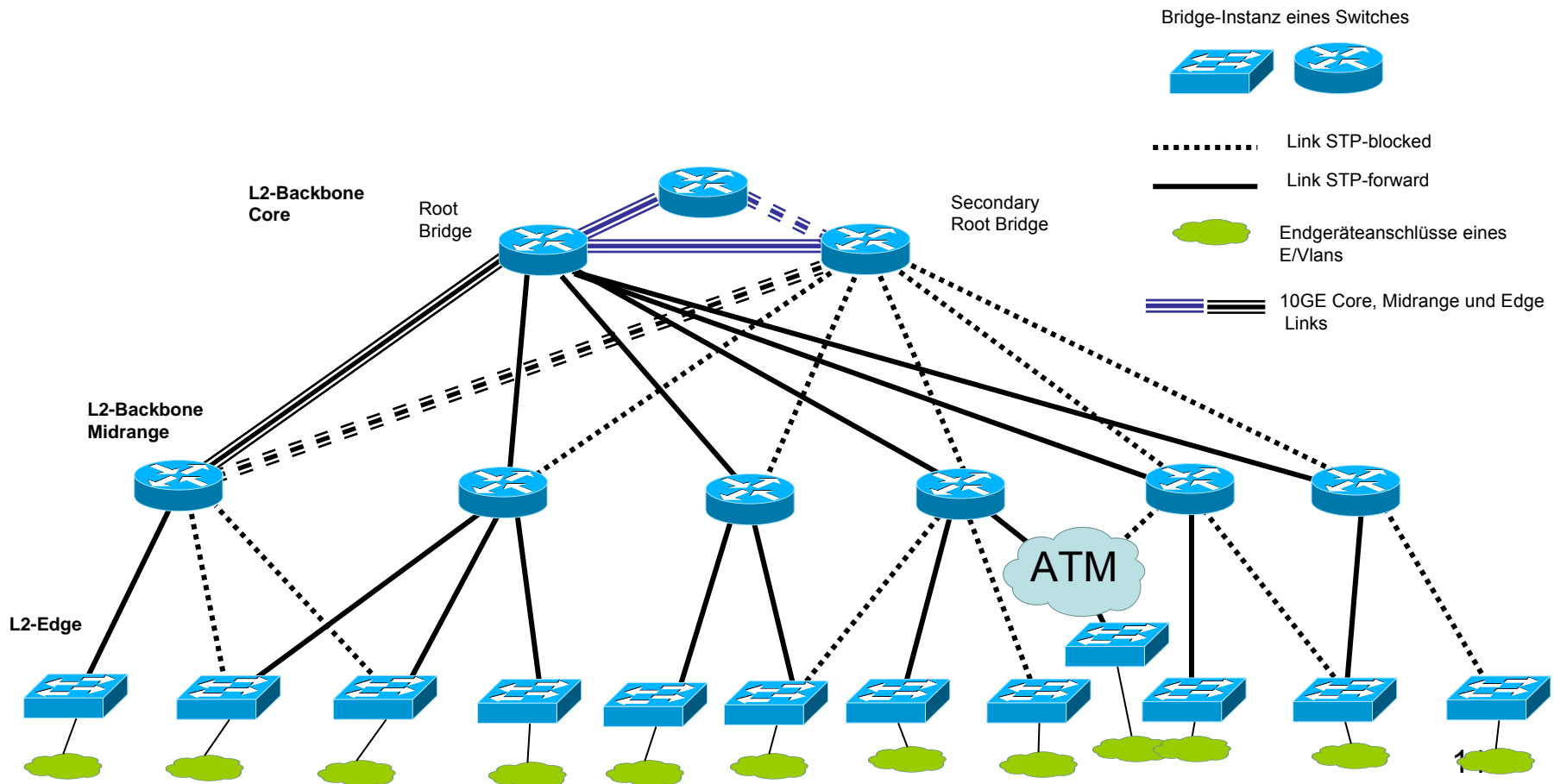
- analoge Einbindung in Netzzonen

Erweitertes technisches Konzept

- Technik-Ersatz und -Ergänzung durch
 - Virtuelle Router (mit ACLs)
 - Virtuelle Firewalls
(stateful packet screening, port agil)
 - Virtualisierte VPN-Zugänge in beliebige Zielnetze,
voll routing-integriert
 - Virtuelle Intrusion-Prevention-Systeme

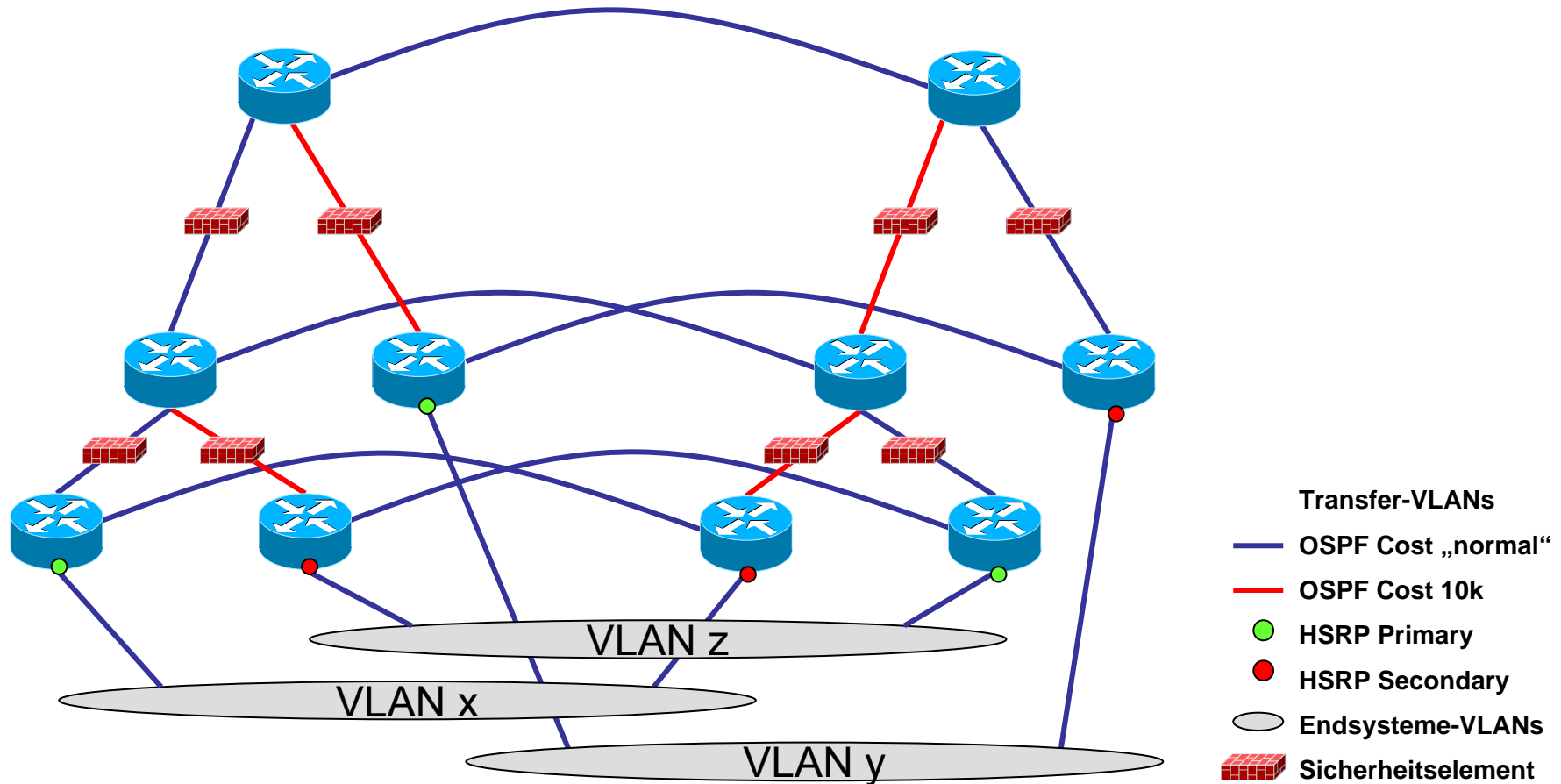
L2-Backbone-Struktur für Endsystem-VLANs

Darstellung für ein VLAN



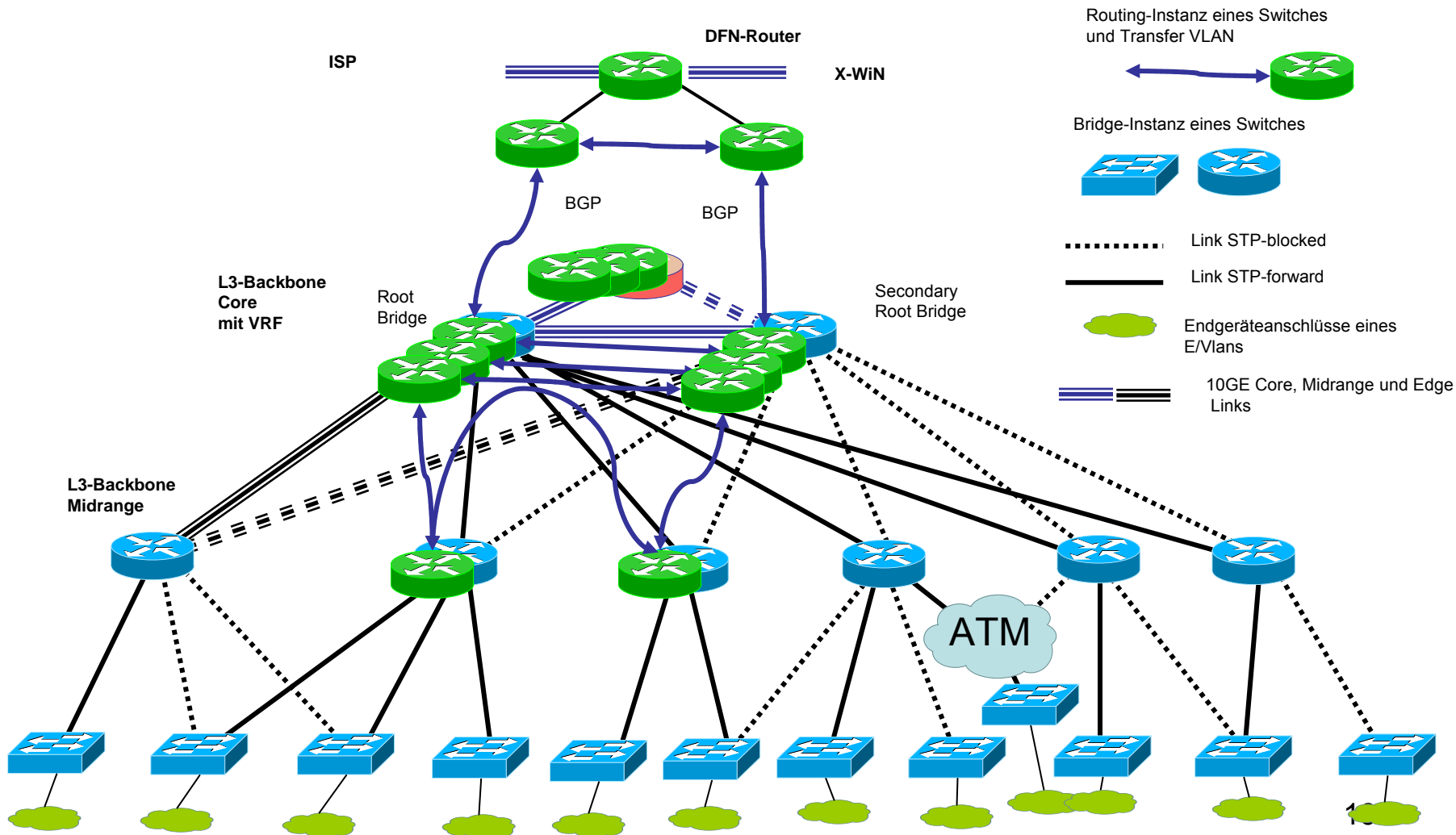
Redundanz und Load-Sharing

- für alle Funktionen (Routing, FW, IPS, ...)



L3-Routing für Endsysteme-VLANs

vereinfachte Darstellung für ein VLAN



Cisco Catalyst 6509



Supervisor Engine 720 (3BXL)

- 40 Gbps/Slot (720 Gbps Crossbar)
- 4-Port 10GE Module unterstützt
- IPv4 routing in hardware, bis 400 Mpps
- IPv6 routing in hardware, bis 200 Mpps
- bis 1M Routen (IPv4), 500k (IPv6)
- bis zu 1024 VRF (virtuelle Router)
- 32k Port-ACLs

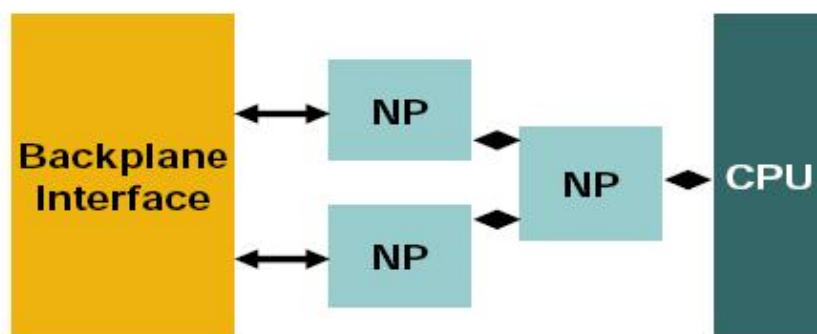
Firewall Services Module Quick Recap...

Cisco.com



THE **WS-SVC-FWM-1-K9** SUPPORTS THE FOLLOWING...

- Fabric line card
- Supported in Cisco IOS and Catalyst OS
- Network-processor based hardware
- Up to 5Gb aggregate throughput
- Up to 3Mpps aggregate performance
- Up to 1M TCP concurrent connections
- Supports dynamic routing (OSPF)
- Up to 100K new connections per second for HTTP, DNS and enhanced SMTP
- Support for 100 Virtual Firewalls
- Transparent Firewall support
- Intra and Inter chassis failover in Active/Standby mode
- Dynamic Routing with RIP and OSPF



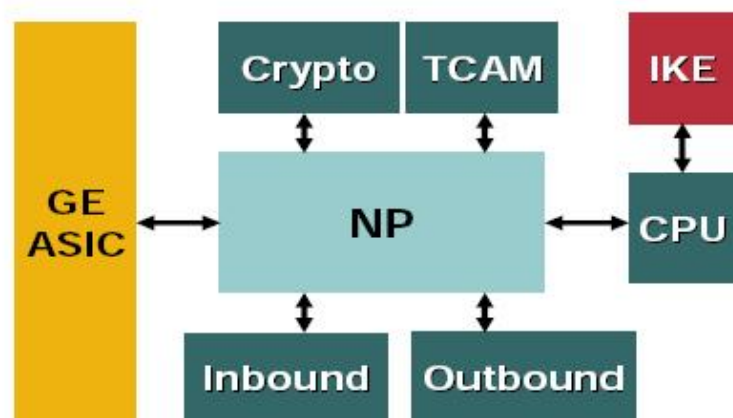
VPN Service Module Quick Recap...

Cisco.com



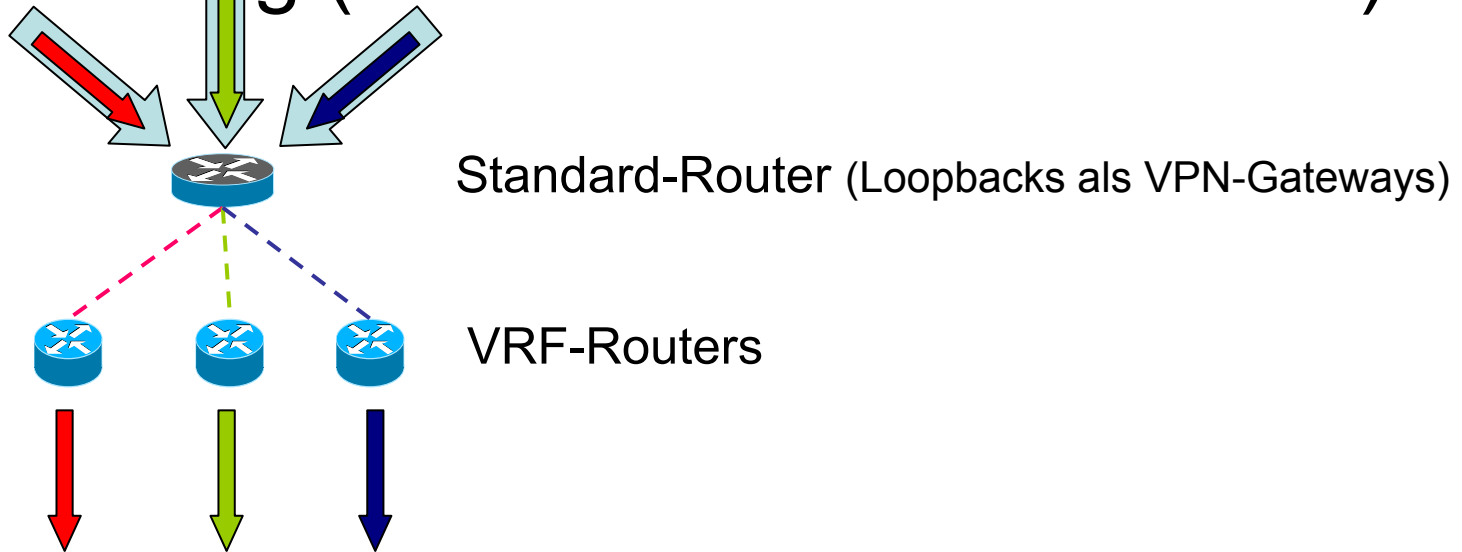
THE **WS-SVC-IPSEC-1** SUPPORTS THE FOLLOWING...

- Supports connection to 32-Gbps shared bus
- Supports single 8-Gbps fabric connection
- Cisco IOS® support only
- Sup2 and Sup720 support
- IPsec site to site VPN
- EZ-VPN Client support
- Up to 8000 tunnels supported
- 1.9Gbps 3DES performance (500+ byte packets)
- 1.6Gbps 3DES performance (300+ byte packets)
- Tunnel setup rate 60 tunnels/sec
- IKE, IKE-XAUTH, MD5, SHA-1, SSH
- Kerberos Telnet, X.509 Digital signatures
- Shared Secrets
- ESP DES and 3DES
- ...



VPN-Service-Modul

- VRF-fähig (VRF-aware-IPSec Feature)

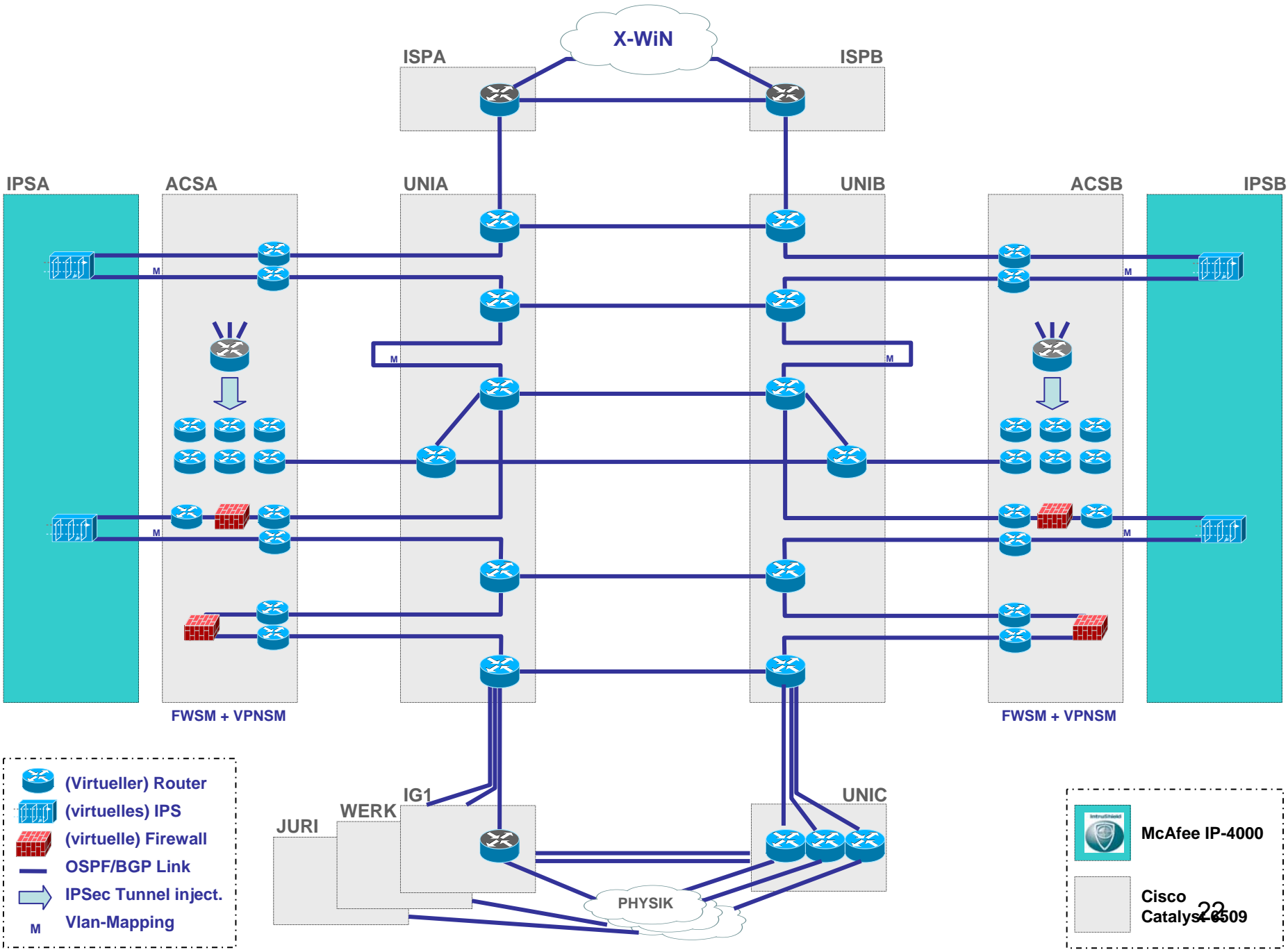


- virtuelles Tunnelende auf beliebigem VR (in gleichem Chassis), d.h. mandantenorientiert
- volle Routing-Integration
- nur der Standard-Router zur Anbindung der IPSec-Tunnel

McAfee Intrushield 4000



- IPS: Intrusion Detection und Prevention
- signaturbasiert, verhaltensbasiert, kombiniert
- Blockierung in Echtzeit (nach Bedarf)
- bis zu 2 Gbit/s Performance (1 Gbit/s full duplex)
- bis zu 1000 virtuelle Systeme
- mandantenfähiges Management

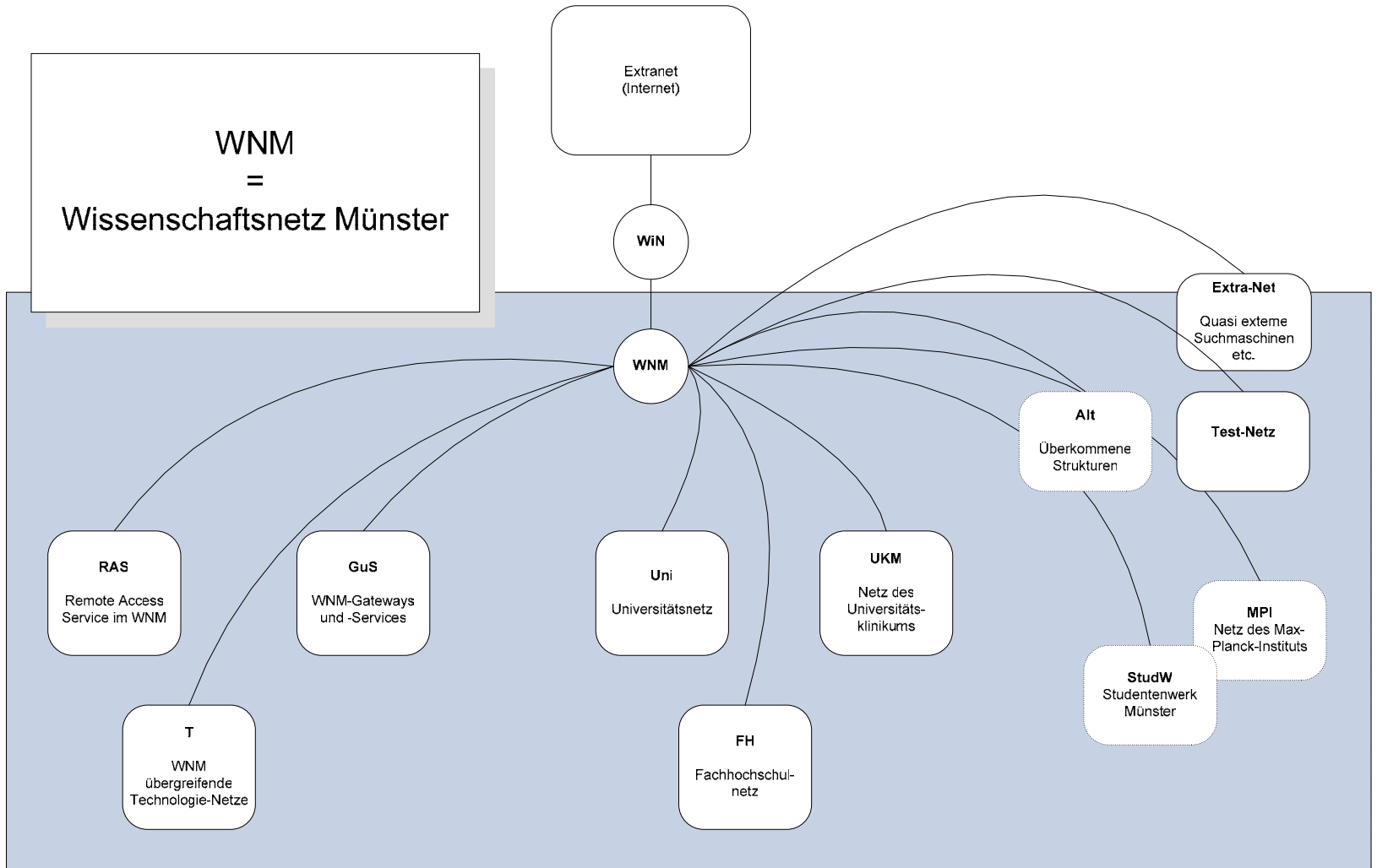


Integrierte Sicherheit in Strukturierten Netzen

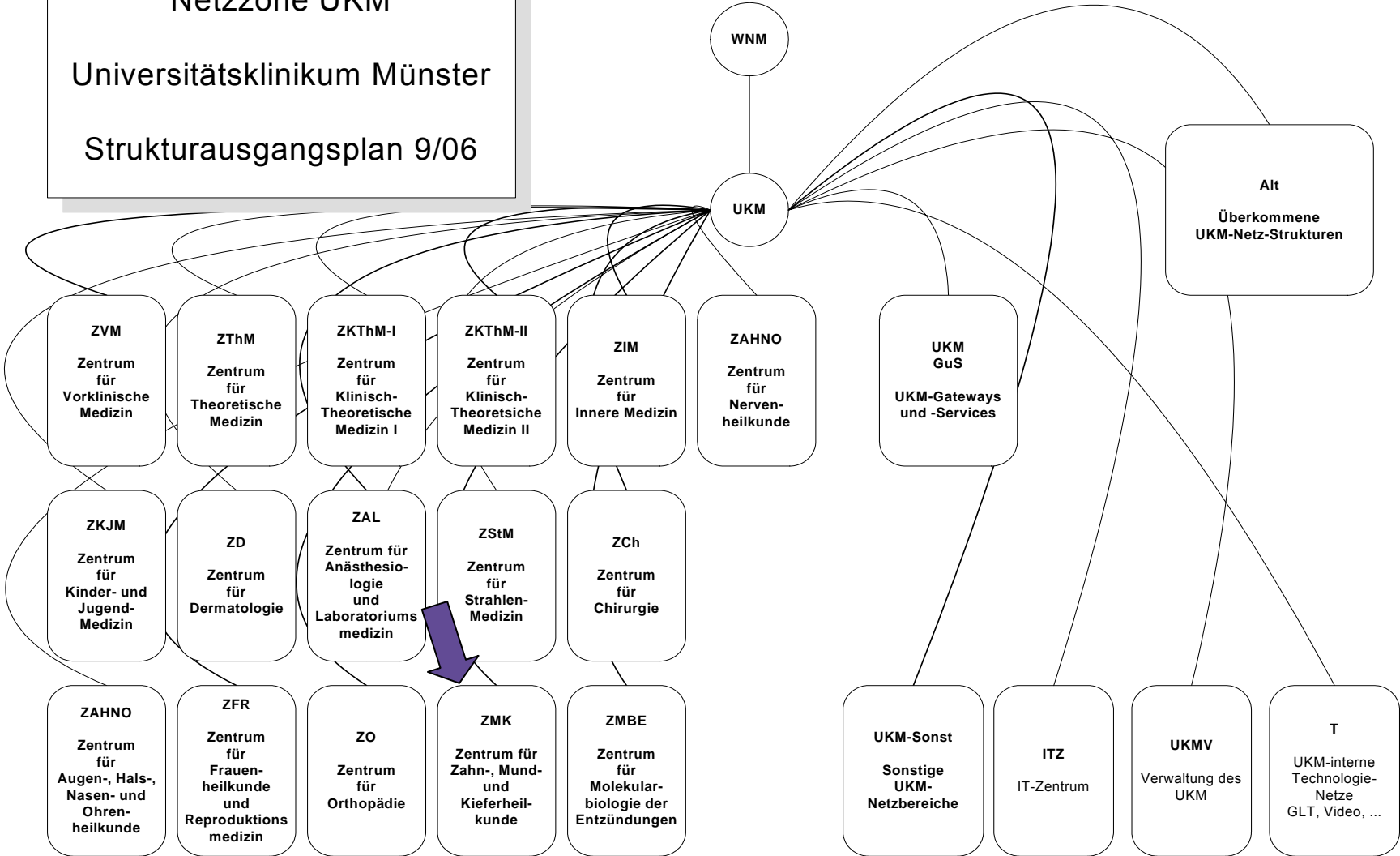
Virtualisierung
von
Netzstrukturen und Sicherheitselementen
in
Lokalen Rechnernetzen

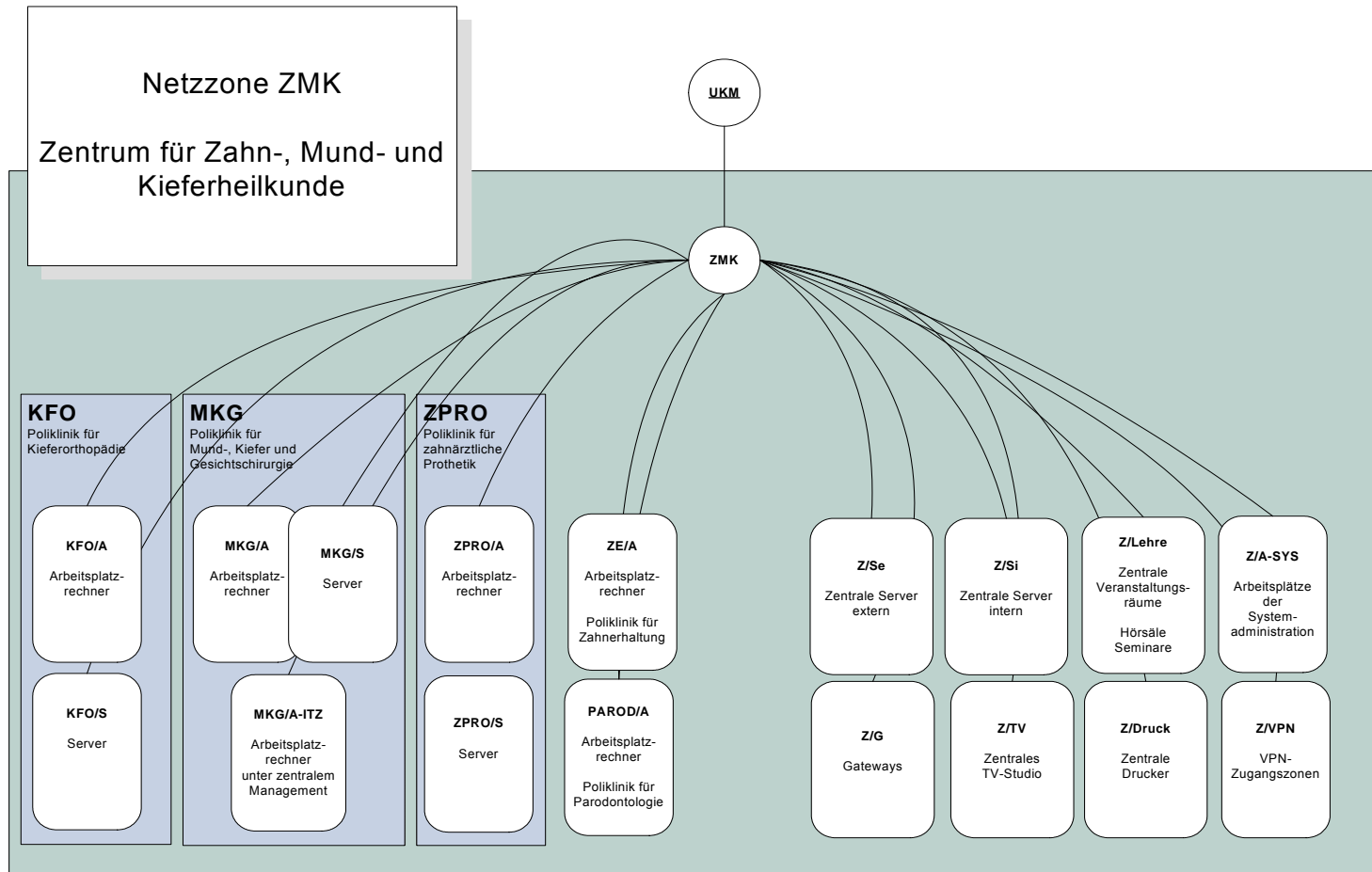
- *Grundlagen*
- *Implementierung*
- *Strukturen*
- *Organisation*



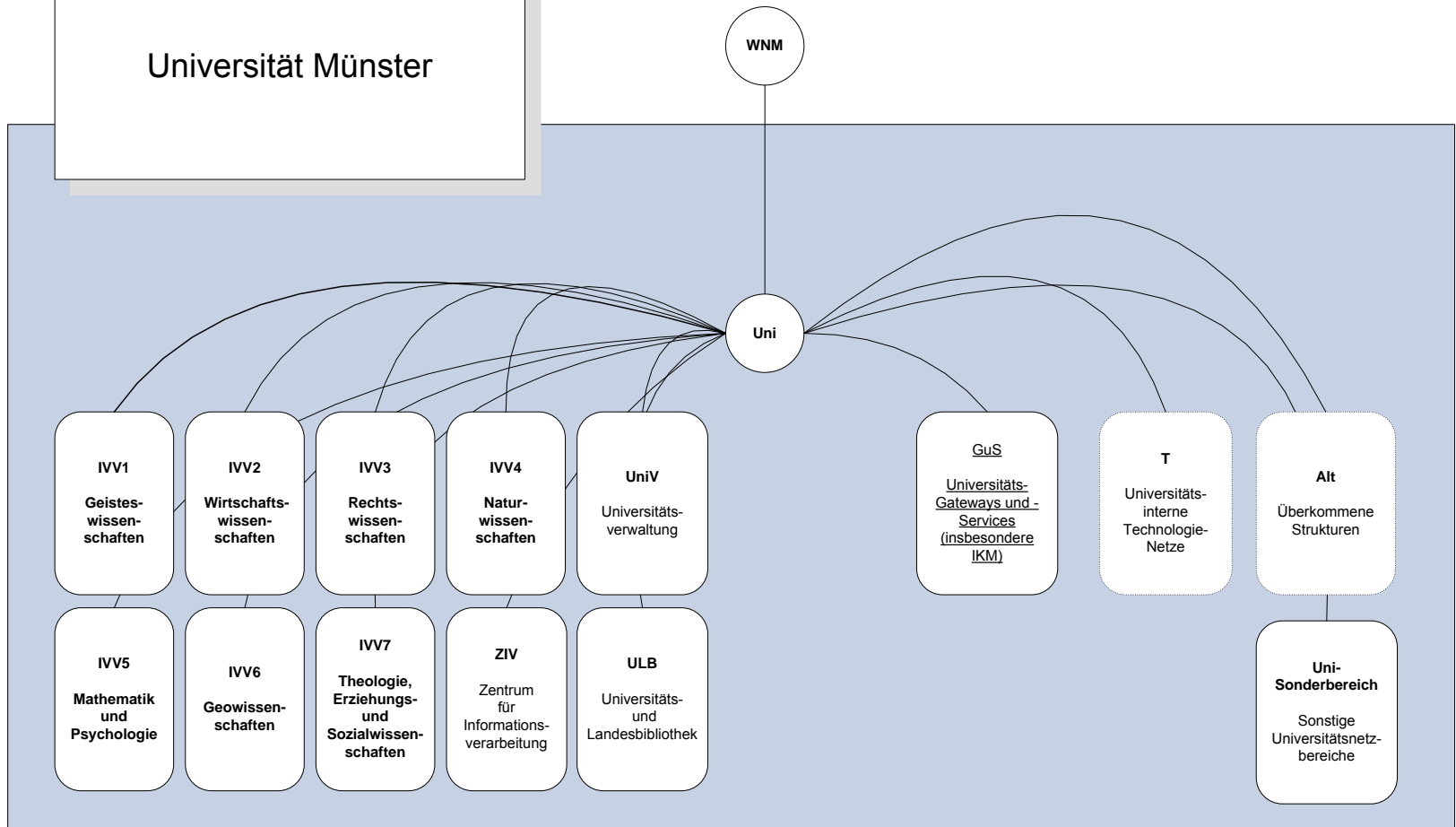


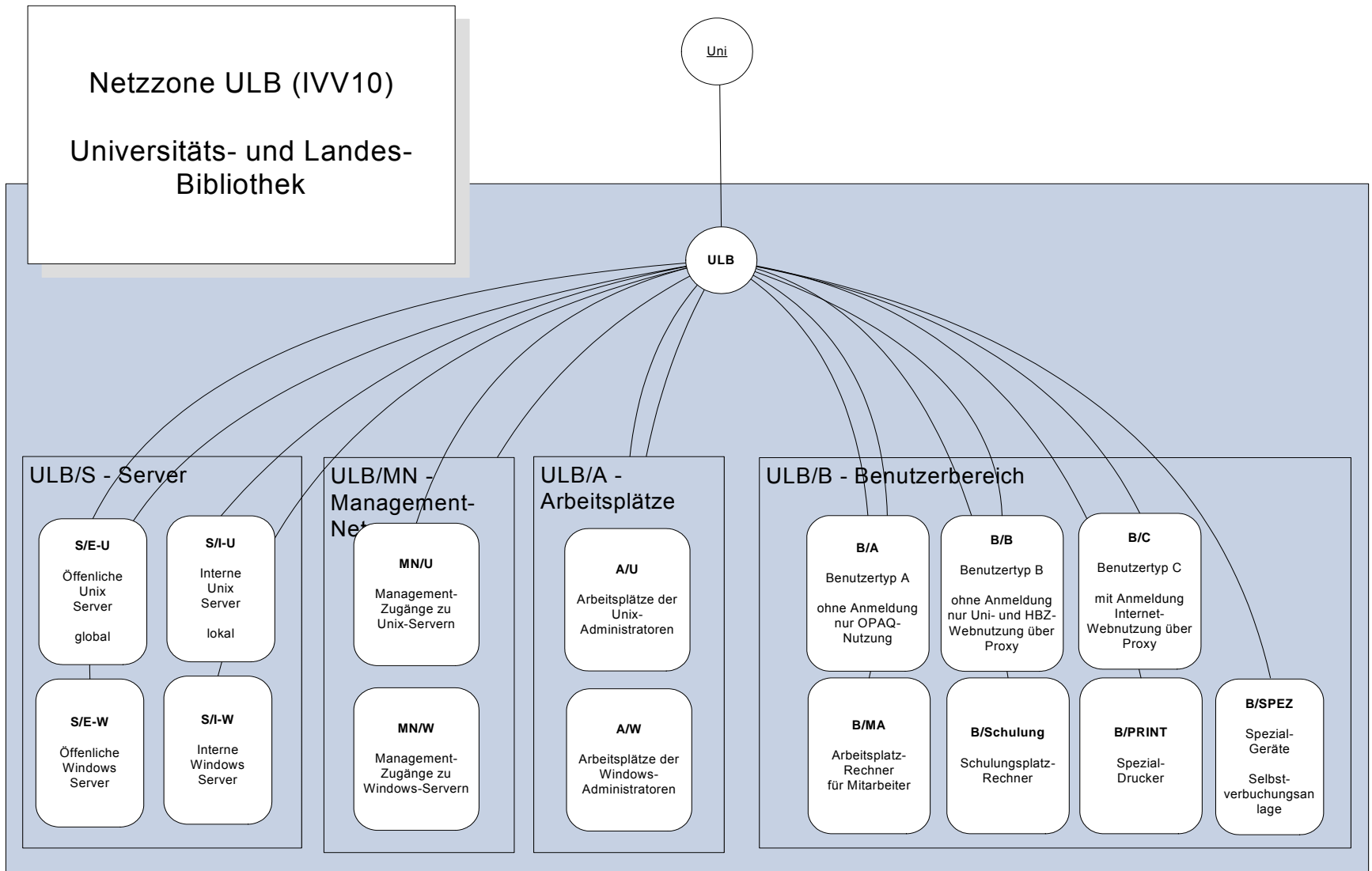
Netzzone UKM
Universitätsklinikum Münster
Strukturausgangsplan 9/06

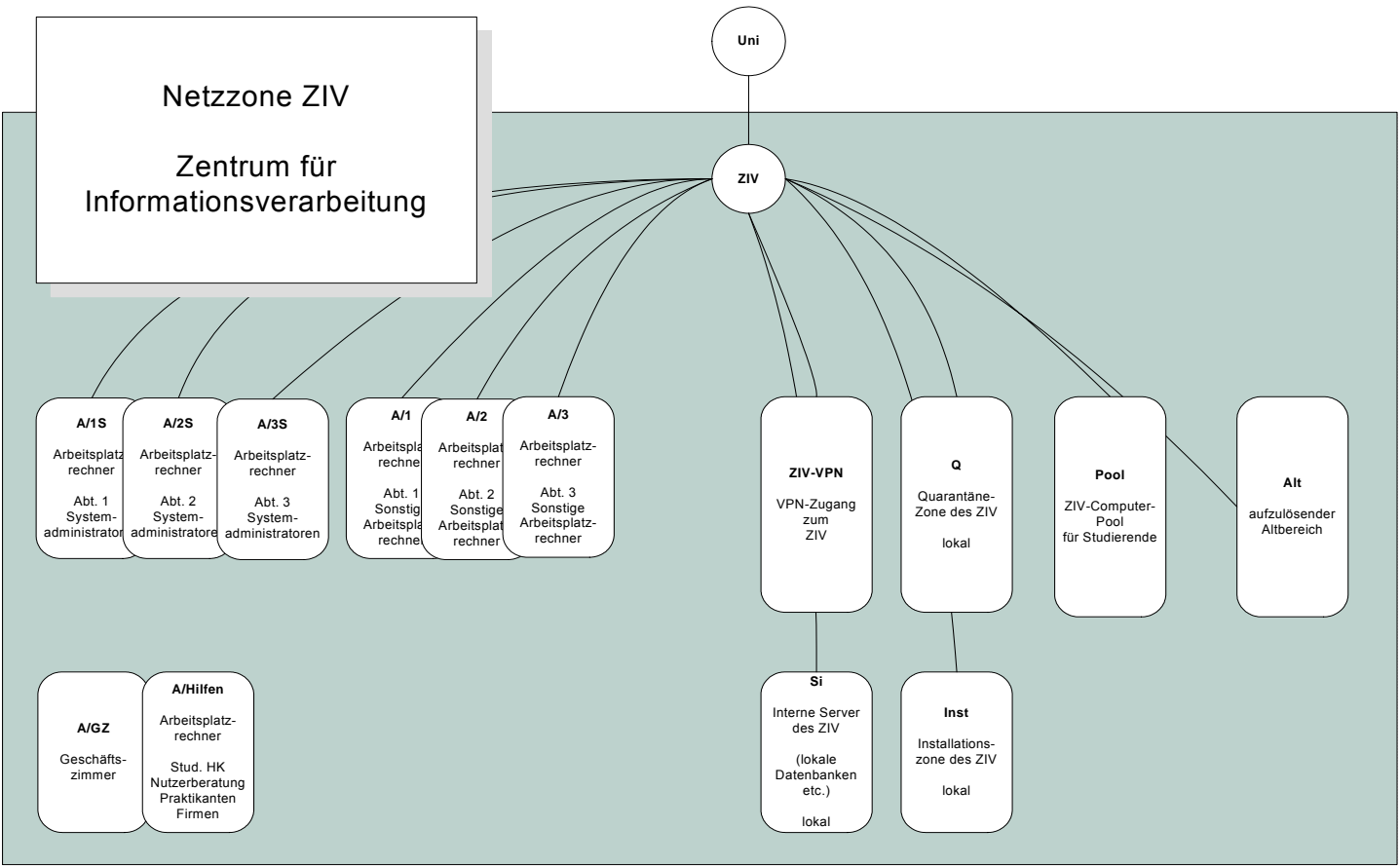




Netzzone Uni
Universität Münster

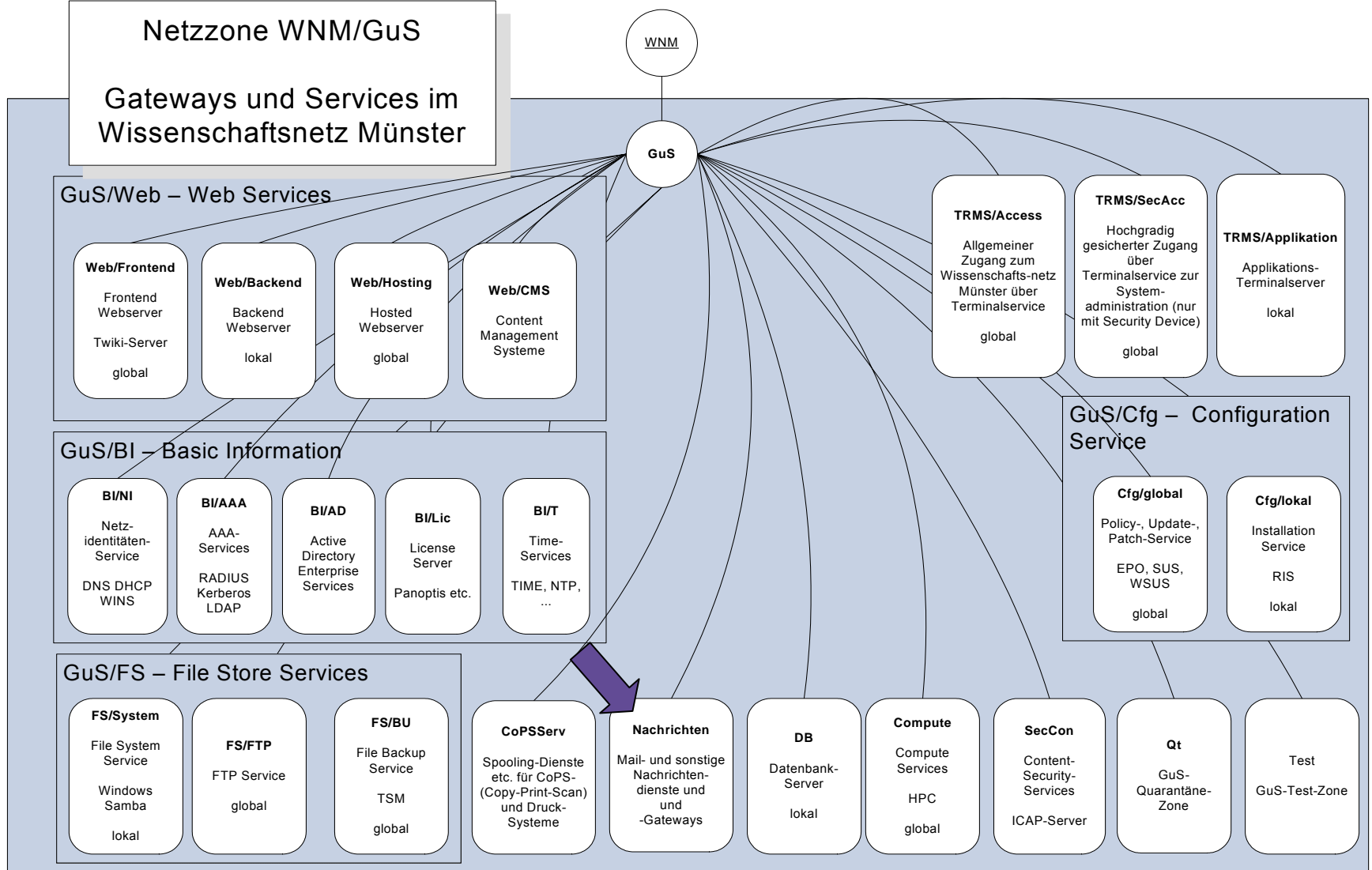




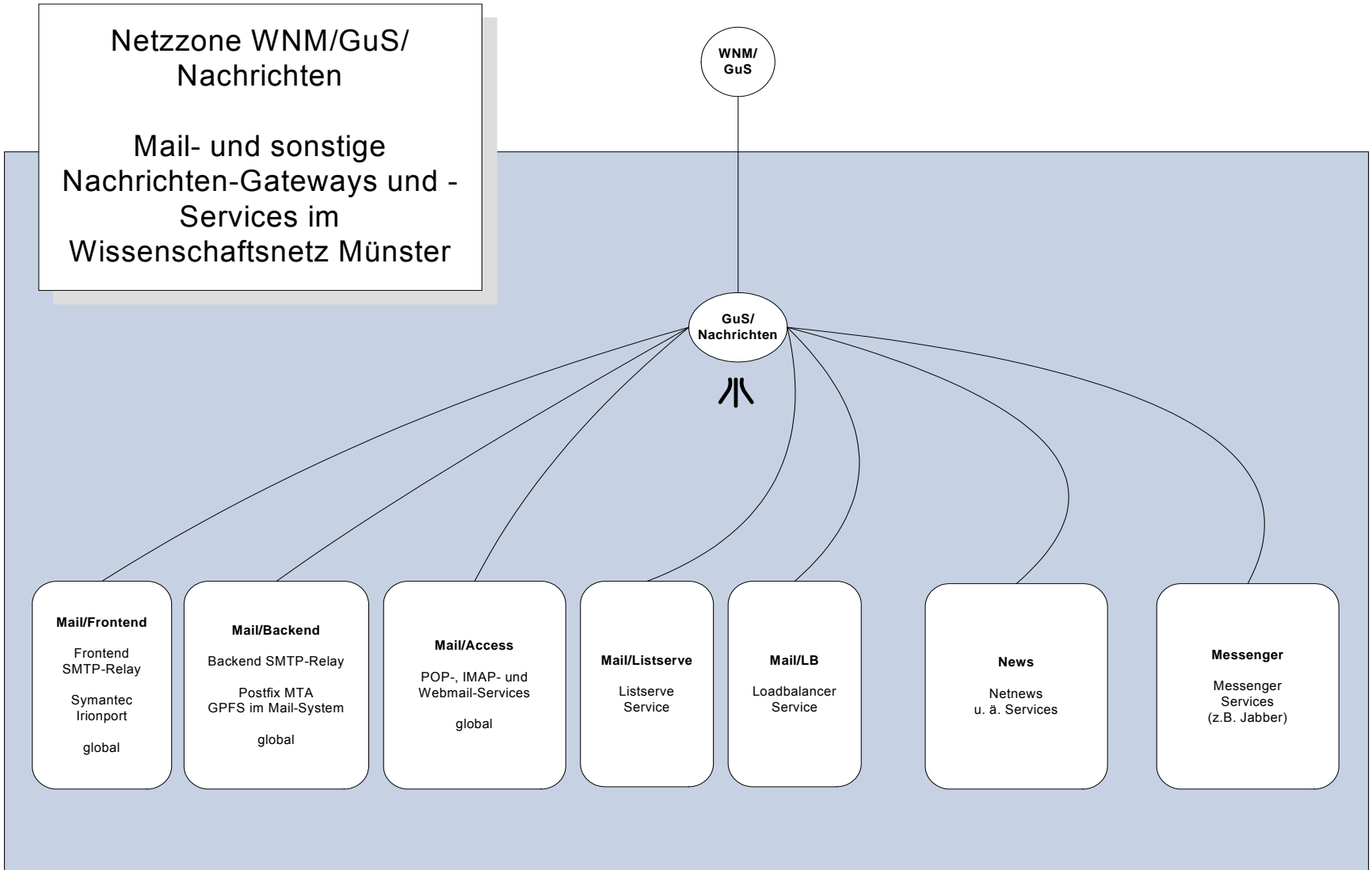


Netzzone WNM/GuS

Gateways und Services im Wissenschaftsnetz Münster

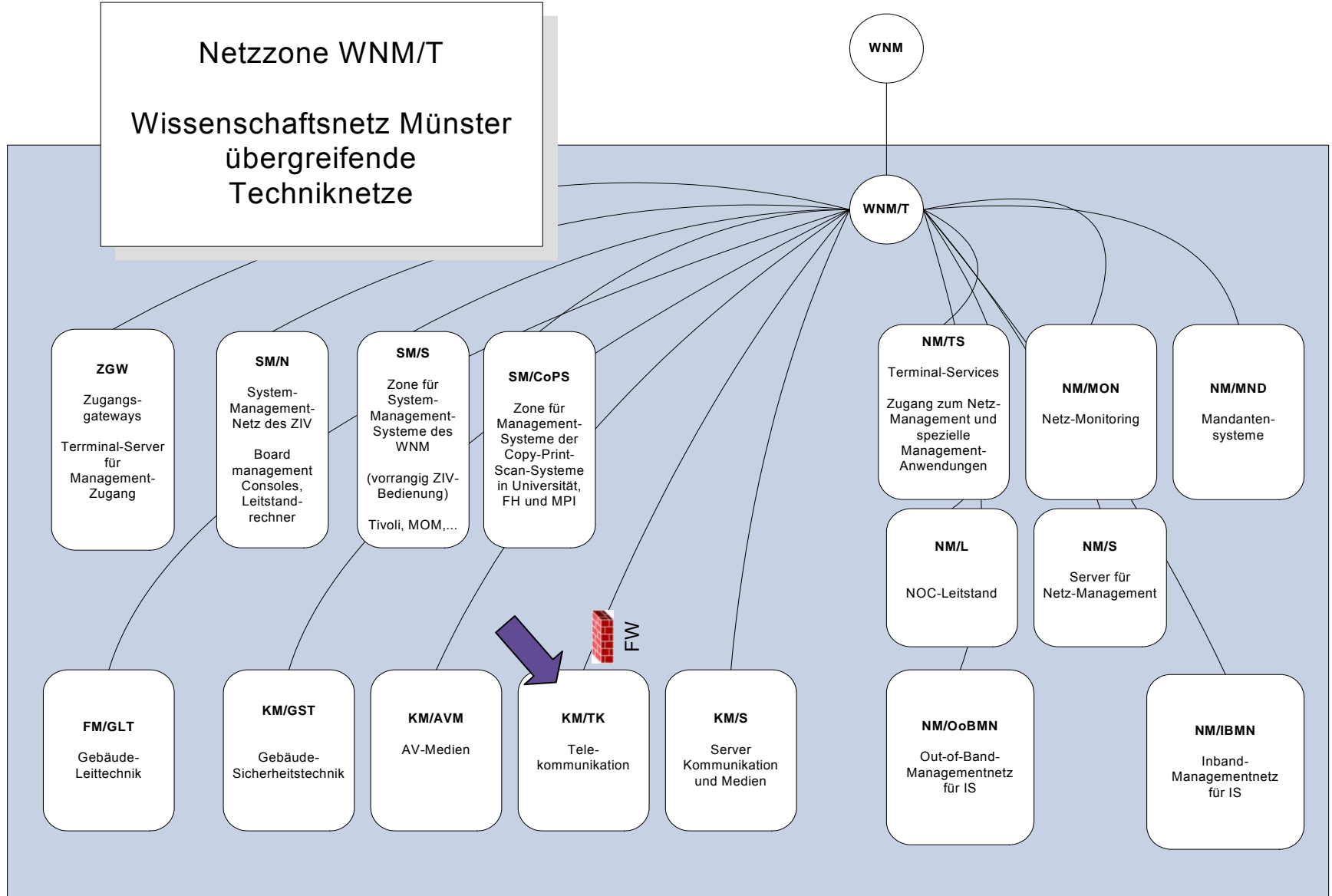


22.01.07



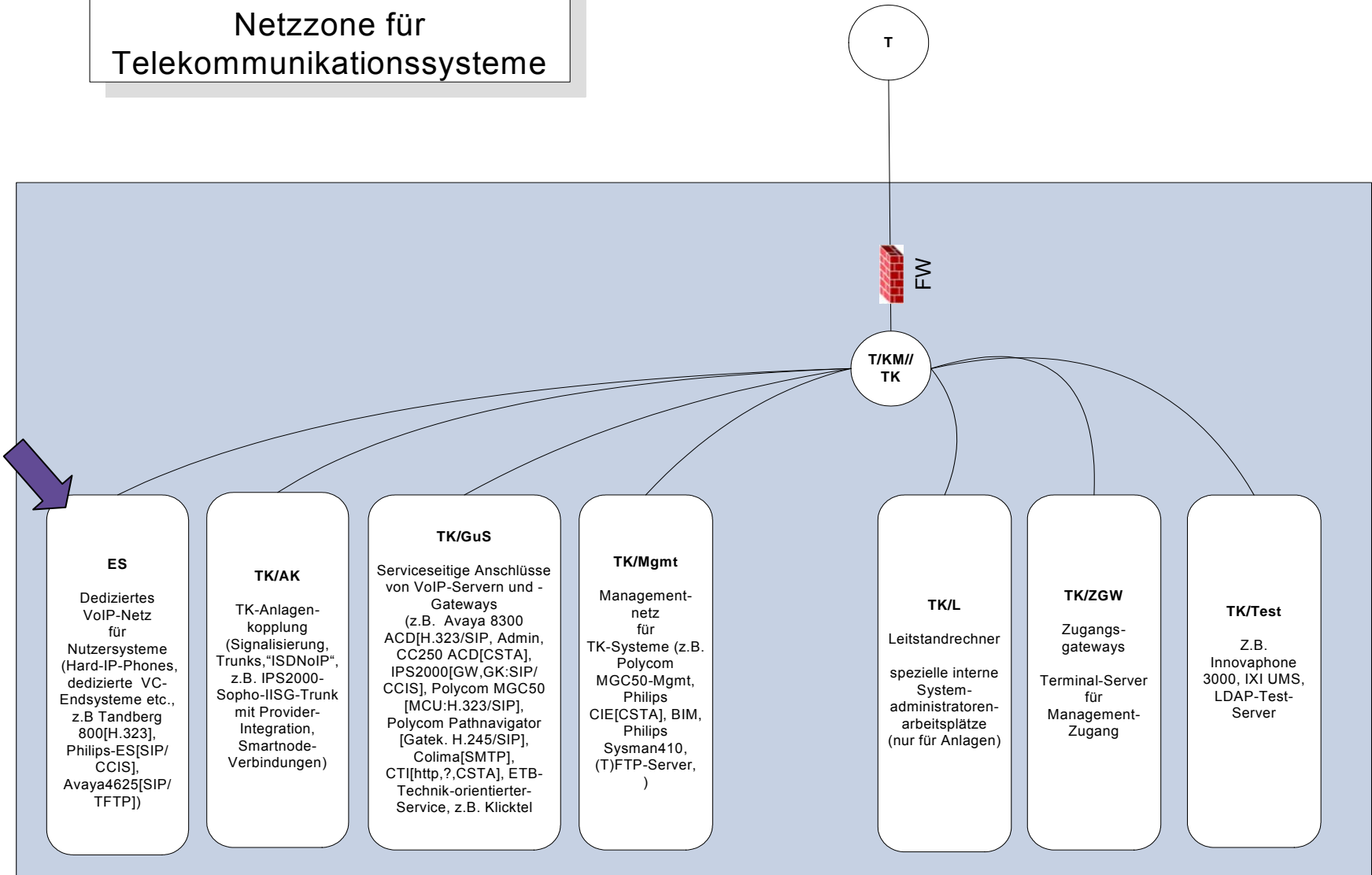
Netzzone WNM/T

Wissenschaftsnetz Münster übergreifende Techniknetze



WNM/T/KM/TK

Netzzone für Telekommunikationssysteme



Netzzone WNM/T/TK/ES

Dedizierte Netzzone für
Telekommunikations-
Endsysteme

