



Virtuelle Firewalls im Münchner Wissenschaftsnetz (MWN)

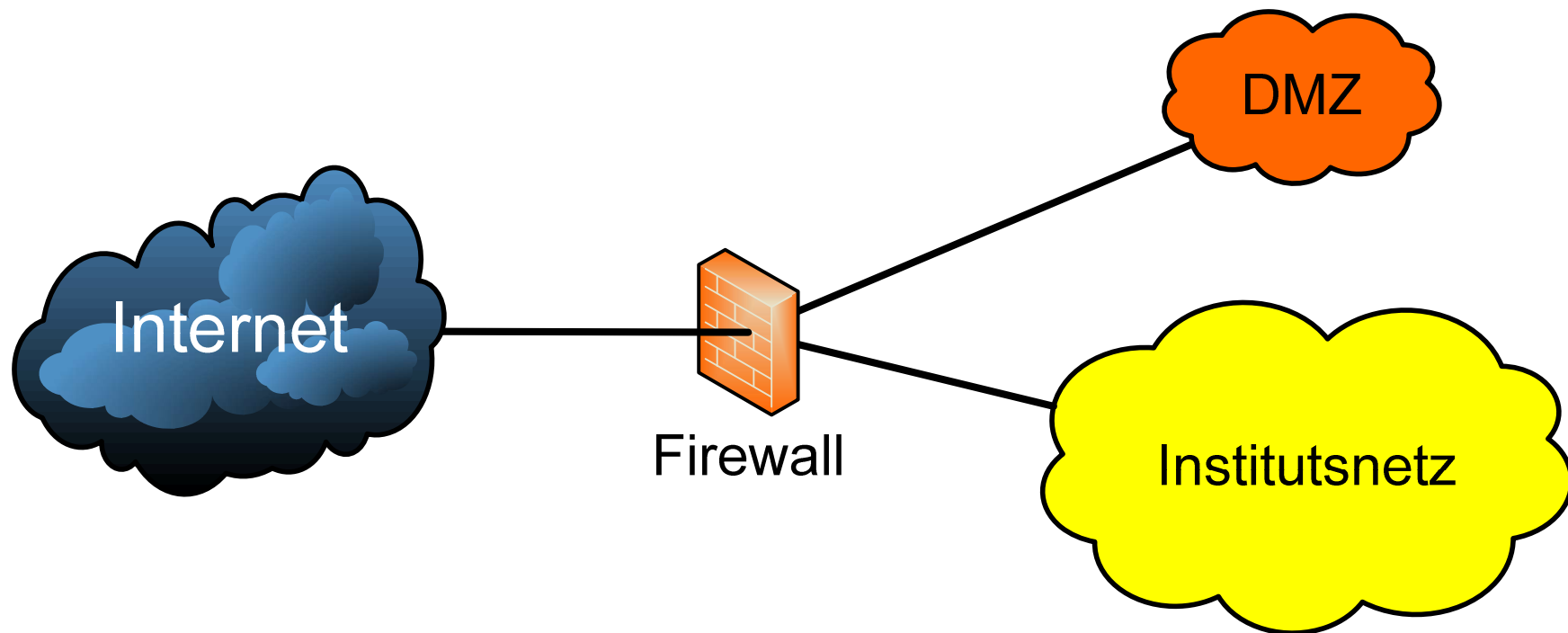
Ralf Kornberger, Claus Wimmer

Firewall: Brandmauer für das Institutsnetz



- ❑ **Typen**
 - Appliance (z.B. Cisco Pix)
 - Software (z.B. Astaro, MS ISA Server)
- ❑ **Filter**
 - Stateless versus Stateful
- ❑ **Betriebsmodi**
 - Routed versus Transparent (Bridging)
- ❑ **Total Cost of Ownership (TCO)**
 - Anschaffung
 - Installation
 - Wartung (Software, Hardware)
 - Betrieb (Konfiguration, Logging)

Typisches Firewall-Setup



Virtuelle Firewall: Vorteil



- ❑ **Vollwertiger Ersatz für Appliance (Cisco PIX Derivat)**
- ❑ **Übliche Setups und Architekturvarianten möglich**
 - Internet – Mitarbeiternetz (Dual Homed/Bastion Host)
 - Internet – Mitarbeiternetz – DMZ/Server-Netz (Screened Subnet)
 - ...
- ❑ **LRZ-Service**
 - Anschaffung
 - Installation
 - Wartung (Software, Hardware)
- ❑ **Total Cost of Ownership (TCO)**
 - Betrieb (Konfiguration, Logging)

Virtuelle Firewall: Die Hardware



- ❑ **Firewall-Blades**
 - Zusatzmodule für Cisco-Router
- ❑ **Leistungsmerkmale pro Modul**
 - Gesamte Datenübertragungsrate: ca. 6 Gbit/s
 - Anzahl virtueller Firewalls: maximal 250
 - Filterregeln: ca. 11.000
- ❑ **Aktuelles System**
 - 5 + 1 Module
 - 20 virtuelle Firewalls pro Modul
- ❑ **Ausfallsicherheit**
 - „Cold Standby“: Im Schadensfall Austausch des defekten Modules mit Reserve-Modul
 - Perspektive: High Availability durch redundante Module pro Router

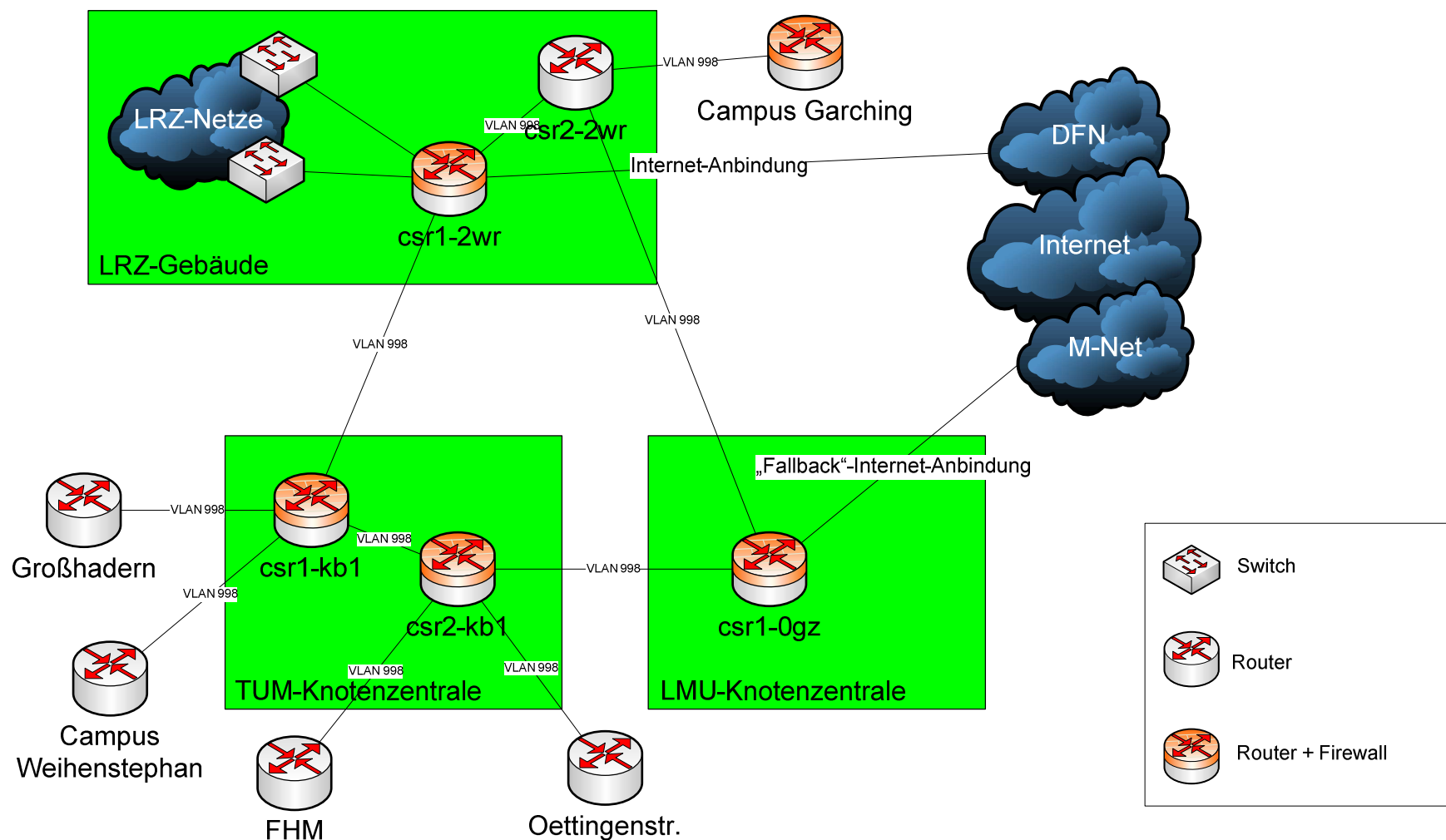
❑ **Backbone-Router**

- Core-Router im Dreieck (z.B. LMU Knotenzentrale)
 - Direkt angeschlossene IP-Netze
 - Weitere(r) Router
- Distribution-Router am Rand (z.B. Campus Garching)
 - Direkt angeschlossene IP-Netze

❑ **Ausstattung mit Firewall-Modulen**

- 4 Core-Router, 1 Distribution-Router
- LRZ (1, Core),
LMU Stammgelände (1, zukünftig 2, Core),
TUM Stammgelände (2, Core),
Campus Garching (1, Distribution)

Das MWN-Backbone

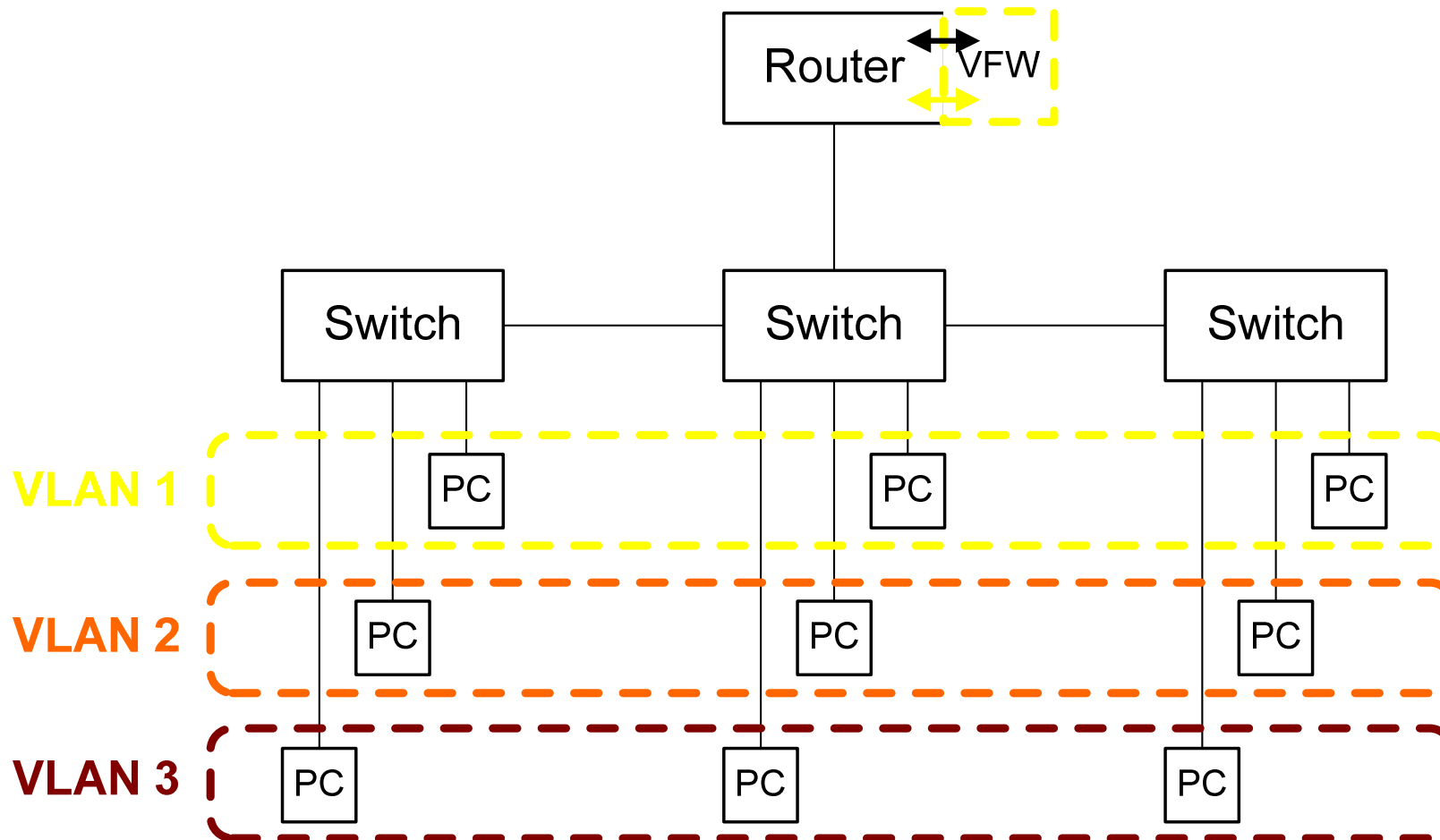


Virtual Local Area Network (VLAN)



- ❑ **Institut besitzt ein IP-Subnetz (z.B. 129.187.10.1-254)**
- ❑ **Institut ist historisch gewachsen:**
 - Verteilte Räume, mehrere Stockwerke, mehrere Gebäude
- ❑ **Problem: Zusammenfassen der Datendosen aller Räumlichkeiten in einem LAN**
- ❑ **Lösung A: Ziehen von Kabeln – zu aufwendig!**
- ❑ **Lösung B: Konfiguration eines VLAN**
- ❑ **VLAN ist eine logische Schicht zwischen Kabelnetz und IP-Netz**
 - Trennung des Verkehrs innerhalb des VLANs vom restlichen Verkehr im Kabel (z.B. andere VLANs)
 - Ausdehnung über Switches und Router
- ❑ **Virtuelle Firewall terminiert Instituts-VLAN**
 - Definierter Übergang zum MWN

VLAN



Verwaltung einer virtuellen Firewall



- ❑ **Adaptive Security Device Manager (ASDM)**
 - Web-Interface: Java Applet
 - Funktionsumfang: Teilmenge der verfügbaren Features, meistens ausreichend (prominente Lücke: IPv6)
 - Zielgruppe: Lokaler Verwalter, Globaler Verwalter (LRZ)
- ❑ **Secure Shell (SSH)**
 - Command Line Interface (CLI): Cisco IOS Style
 - Funktionsumfang: Alle verfügbaren Features
 - Zielgruppe: Lokaler Verwalter, Globaler Verwalter (LRZ)
- ❑ **Cisco Security Manager (CSM)**
 - MS Windows Client/Server: Zentrales Management-Werkzeug
 - Funktionsumfang: Ausrollen neuer virtueller Firewalls, Versionskontrolle und Backup der Konfigurationen usw.
 - Zielgruppe: Globaler Verwalter (LRZ)

Organisation: Einer für Alle



- ❑ **Aufbau und Betrieb einer virtuellen Firewall setzt mindestens Grundkenntnisse in Datennetzen voraus**
- ❑ **Nur regelmäßige sachkundige Kontrolle der Log-Daten stellt Funktion sicher**
- ❑ **Aufwand durch Aufbau von Knowhow und Personalressourcen für den Betrieb**
- ❑ **Zentrale virtuelle Firewall z.B. für mehrere Lehrstühle**
 - Schont den Ressourcenbedarf
 - Belastet nicht jeden Lehrstuhl
- ❑ **Zentralisierung, die Sinn macht!**

Organisation: Der Netzverantwortliche



❑ Topologie-Voraussetzungen

- Strukturierte Verkabelung (Switches, kein Koaxkabel)
- Prinzip: 1 Subnetz pro VLAN
- Subnetz gehört vollständig Institut/Organisation oder Teilhaber sind sich einig

❑ Ansprechpartner für Institut/Organisation: Netzverantwortlicher

- Netzverantwortlicher klärt Topologie (bei Bedarf zusammen mit Arealbetreuer im LRZ)
- Falls Voraussetzungen erfüllt sind:
Netzverantwortlicher löst per E-Mail an firewall@lrz.de
die Einrichtung der virtuellen Firewall aus

Weitergehende Informationen



- ❑ **Dokumentation und FAQ**
<http://www.lrz-muenchen.de/services/security/virtuelle-fw/>
- ❑ **E-Mail-Verteilerliste**
fw-mwn@lists.lrz-muenchen.de
- ❑ **E-Mail-Adresse Service**
firewall@lrz.de