

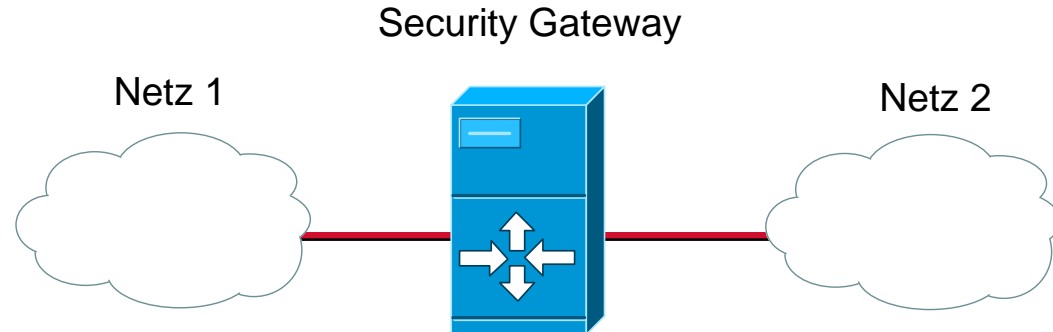
Security Gateway

Michael Stocker

Bernhard Wintersperger

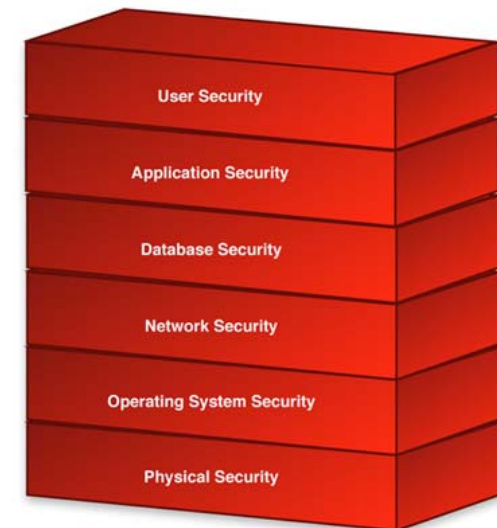
Allgemeines

- **Betreuer:** Dipl.-Ing. Dr. techn. Franz Pucher
- **Sichere Grenze zwischen zwei Netzen**
- **Security Policy**
- **Open Source**



Security Policy

- **Erstes Teilziel der Diplomarbeit**
- **Allgemeine Definition der Spezifikationen**
- **Legt Verhalten des Gateways fest**



Kunden und Anwender

- **Kunden:** Theoretisch jede Firma/Privathaushalt mit Netzwerk und Sicherheitsbedürfnis
- **Anwender:** Techniker oder versierte Endbenutzer



Marktsituation

- **Hart umkämpfter Markt**
- **Professionelle Produkte**
- **Semiprofessioneller Bereich**
- **Kosten**



Anforderungen

- **Absicherung des Grundsystems**
- **Virtualisierung**

- **Sichere Trennung zweier Netze**
- **Überwachung des Netzwerkverkehrs**
- **Log – Management**

Kernel / Virtualisierung

- **Härtung des Linux Kernels**
- **Rasches Disaster Recovery durch Virtualisierung**



Firewall

- **Definition möglichst effizienter Firewall Regeln**
- **Kein direkter Datenverkehr zwischen den Angeschlossenen Netzwerksegmenten**
- **iptables**

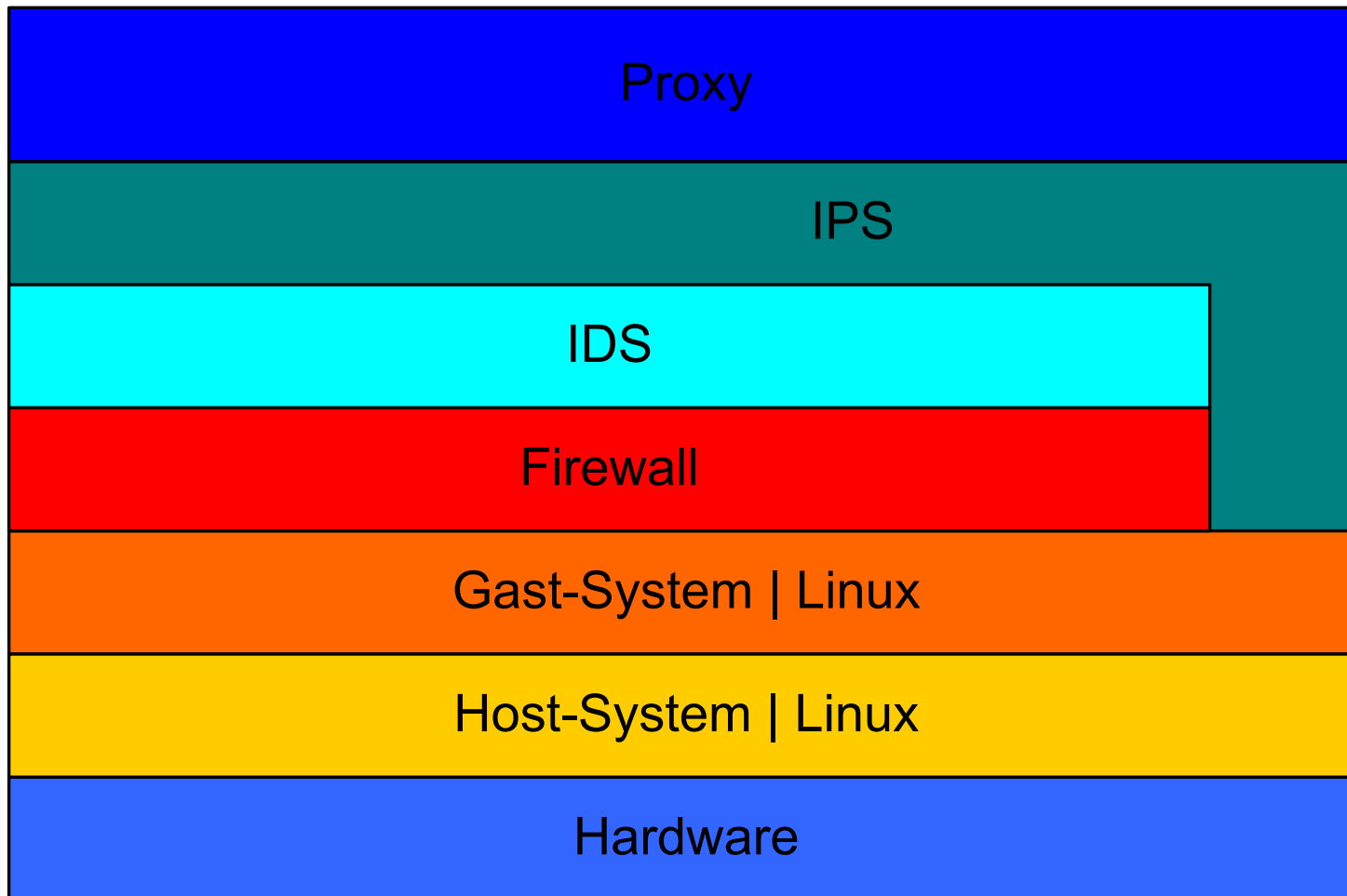


IDS / IPS

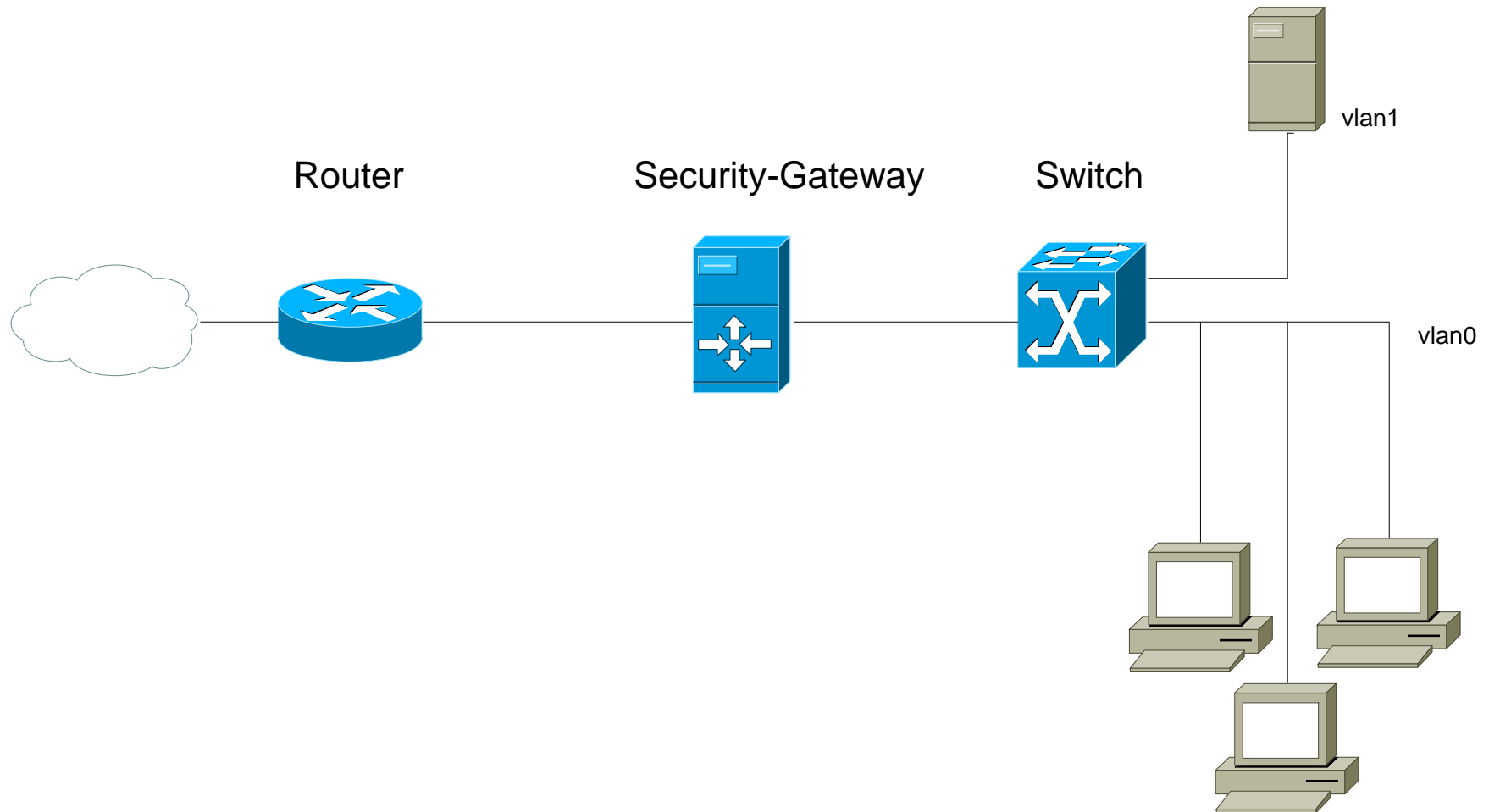
- **Intrusion Detection System**
- **Intrusion Prevention System**
- **Erkennung und Protokollierung von Bedrohungen und Angriffen**
- **Automatisierte Reaktion auf Angriffe**
- **SNORT**



Systemaufbau



Versuchsaufbau



Thank you for your attention!