High Speed Firewalls

Frank Brüggemann

Rechen- und Kommunikationszentrum RWTH Aachen

brueggemann@rz.rwth-aachen.de

High Speed Firewalls

- Anforderung: Durchsatzraten im Multigigabitbereich
- Getrieben durch eine Reihe von Communities (LHC...)

- Nutzung von 10 Gigabit Ethernet
- Integration in entsprechend leistungsfähige Netzwerkinfrastruktur

High Speed Firewalls

- Stand RWTH Aachen Anfang 2006:
- Uplink zum DFN-Verein 1 Gbit/s
- Softwarebasierter zentraler Firewallcluster (Stonesoft) in 1 GbE, 4 Knoten
- Traffic: 400 Mbit/s in, 200 Mbit/s out
- Commitment durch den Fachbereich Physik im Rahmen des LHC-Experimentes: 2 Gbit/s

- Ausbau der Infrastruktur in 10 GbE

High Speed Firewalls

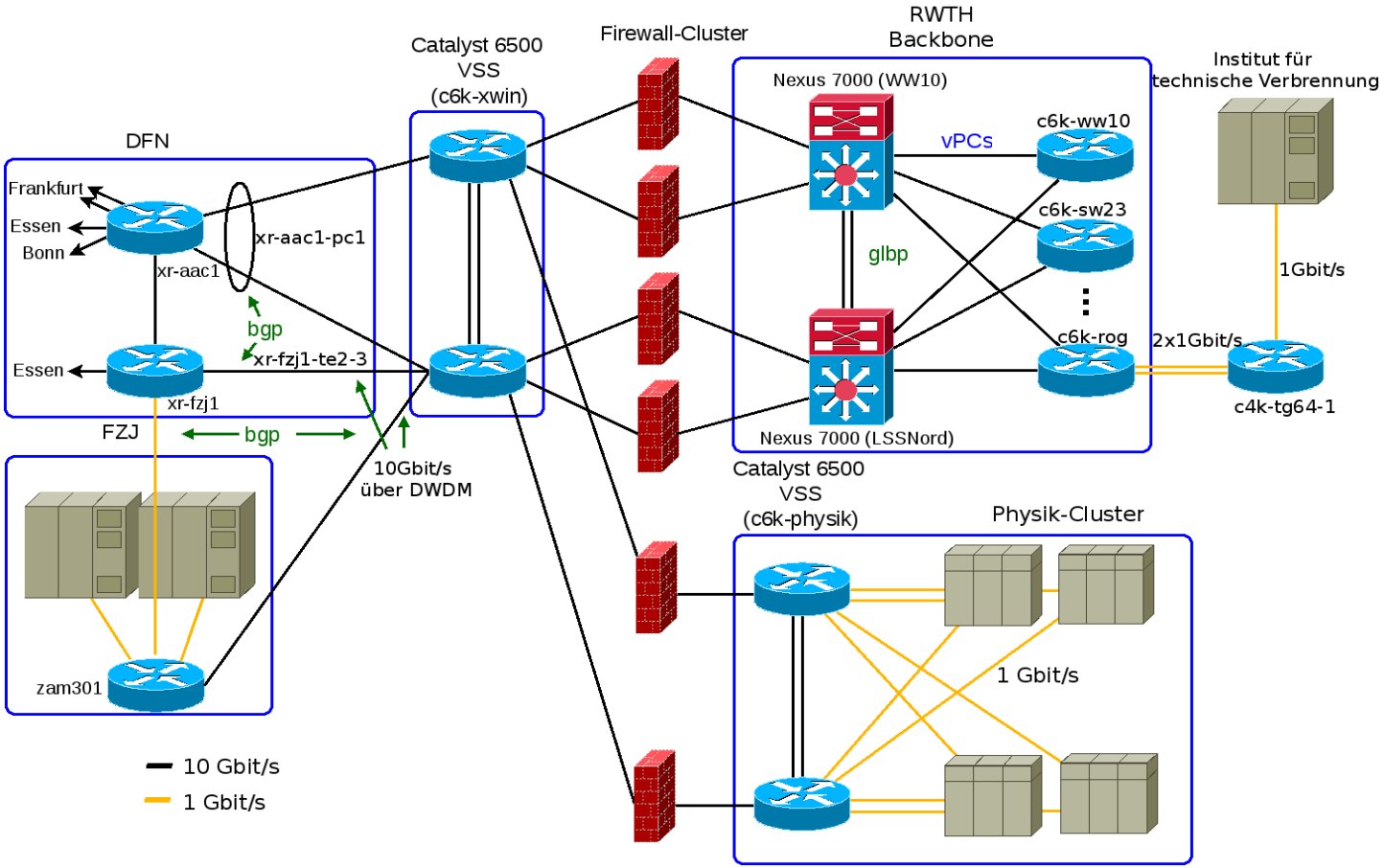
- September 2010:
- Uplink zum DFN-Verein mittlerweile 20 Gbit/s
- Zentraler Firewallcluster (4 Knoten, Stonesoft) in 10 GbE, softwarebasierte Lösung, eigene Hardware, mehrfach migriert
- Linux-Kernel
- PCI Express NICs mit Intel-Chipsatz
- Xeon X5460 @ 3.16 GHz
- State Sync und Heartbeat über dedizierte 1 GbE-Leitungen
- Eingebettet in hochredundante, örtlich verteilte Netzwerkinfrastruktur (Cisco Nexus 7000, migriert von Cisco Catalyst 6500 VSS)

High Speed Firewalls

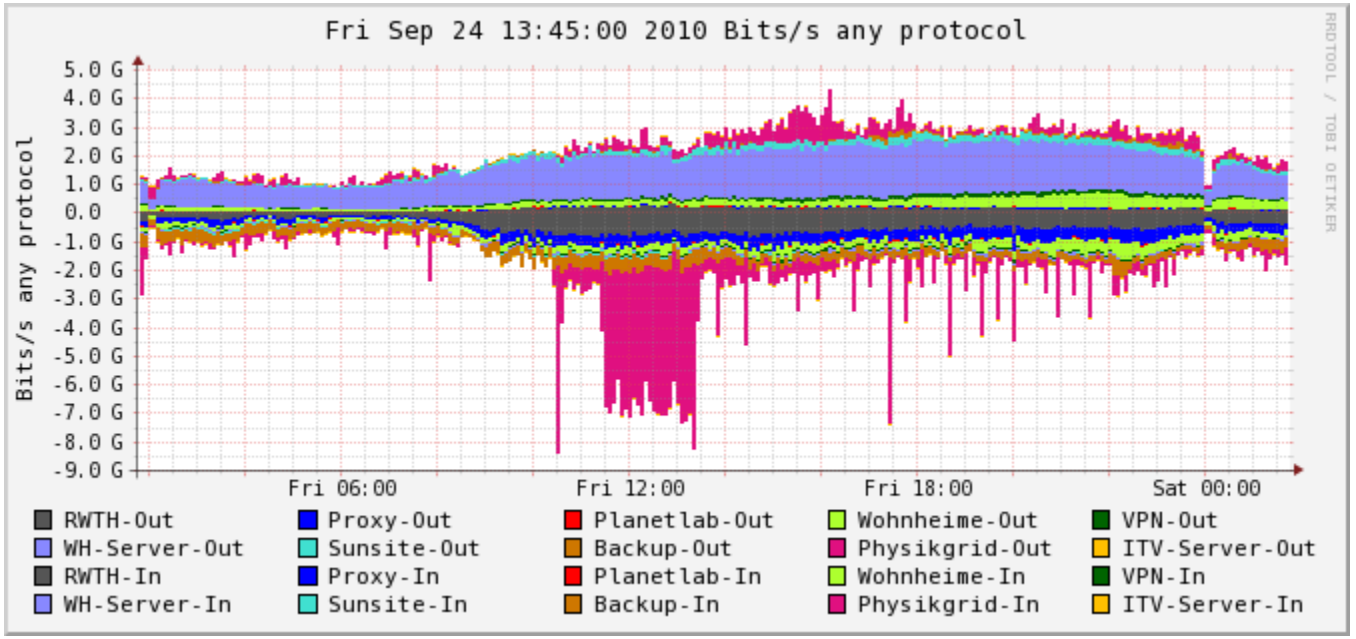
- LHC-Rechencluster abgesetzt in dedizierter 10 GbE-Infrastruktur
- Firewallcluster, 2 Knoten, Stonesoft, Appliances
- Xeon E5450 @ 3.00GHz
- 10 GbE NICs, Intel-Chipsatz, PCI Express
- Redundante Anbindung an Cisco Catalyst 6509 VSS

- Performance-relevante Features für beide Cluster:
- Load Balancing im Cluster über Multicast
- Linux-Kernel verteilt einen Interrupt über mehrere Cores
- 10 GbE-NICs in PCI Express

High Speed Firewalls



High Speed Firewalls



High Speed Firewalls

- **Zentraler RWTH-Firewallcluster:**

- **Komplexe Policy, ca. 60 gefilterte Dienste, bis zu 1.500 angemeldete Server pro Dienst, IP-Bereich umfasst 3 Class-B-Netze**
- **Durchsatz derzeit bis ca. 5 Gbit/s**
- **Latenz ca. 300 Mikrosekunden**

- **LHC-Firewallcluster:**

- **Einfache Policy, kompakter IP-Range, wenige Dienste**
- **Durchsatz bis 9 Gbit/s**
- **Latenz ca. 300 Mikrosekunden**

High Speed Firewalls

- **Mögliche weitere Schritte:**

- **Jetzt:**
- **CPU-Upgrade (Xeon → Nehalem)**
- **Mehr CPUs pro Knoten (skaliert wegen Interrupt-Balancing durch Linux-Kernel)**
- **Mehr Knoten pro Cluster (skaliert wegen Load Balancing via Multicast)**

- **Bald:**
- **Mehrfach 10 GbE pro Knoten durch LACP**

- **Später:**
- **Implementierung neuer Ethernet-Standards (40 GbE oder 100 GbE)**