Westfälische Wilhelms-Universität Münster

Zentrum für Informationsverarbeitung

Embedded Network Security Concept University of Münster

ZIV Lecture
WS 2010/11 – 260068
Münster, December 1st, 2010

Guido Wessendorf
Zentrum für Informationsverarbeitung
Westfälische Wilhelms-Universität Münster
wessend@uni-muenster.de

wissen.leben WWU Münster

topics

Zentrum für Informationsverarbeitung

- security in large networks
  - basic considerations
- concept of Uni Münster
- technical realization
  - routing
  - access control lists (acl)
  - firewall
  - virtual private network (vpn)
  - intrusion prevention (ips)

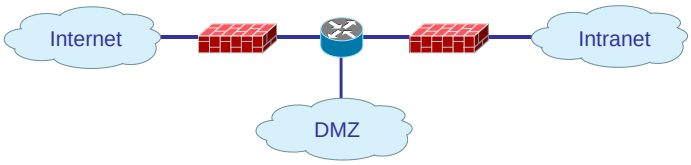
security in large networks

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- how do I increase IT-based security in large complex enterprise networks?
  - precedence: ES security
    - scalable
    - user and application oriented
    - methods (e.g.):
      - anti virus scan
      - personal firewall
      - update services
      - host intrusion prevention
      - policy orchestration
  - network security
  - obvious: task allocation
    - ES administrators:
      - security in ES
      - security in ES applications
      - end-to-end security
    - network administrators:
      - security in transport system (OSI layer 1-4)

„classical“ design insufficient

ZENTRUM FÜR INFORMATIONS VERARBEITUNG



- perimeter firewall absolute insufficient
  - different security requirements within Intranet
  - no protection between Intranet parts
  - complex firewall rules
  - Intranet is as bad as Internet (especially at universities ;-)
  - high Intranet performance may increase efficiency and impact of attacks
- “classical” solution: roll out of many dedicated firewall devices
- problems in large networks
  - management, flexibility, operating and costs
- same considerations for other security instances, e.g. IPS

security concept at Uni Münster (1)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Net Areas ("Netzzonen")
  - basic elements are *Net Areas*
    - grouping of IT-Systems and parts of (network) infrastructure for which the users have common security and/or functional requirements, e.g.
      - workstations
      - servers
      - printers
      - lab systems
      - database systems with confidential information
      - public terminals
  - *Net Areas* can be technically mapped to e.g.
    - virtual LANs (vlans)
    - IP subnets

security concept at Uni Münster (2)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Security for Net Areas
  - securing access to *Net Areas* with embedded network security functions as required, for example by
    - stateless packet screens (Access Control Lists, ACLs on routers)
    - stateful packet inspection (firewalls)
    - application gateways or proxies
    - Intrusion Prevention Systems (IPS)
    - Virtual Private Networks (VPN) technology
    - content filter

security concept at Uni Münster (3)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Structured Network
  - interconnection of *Net Areas* as required, e.g. via
    - routers
    - switches
    - vpn
  - (hierarchical) grouping and interconnection of *Net Areas* analogous to the (hierarchical) organization of enterprise, criteria could be e.g.:
    - rules or responsibilities
    - security requirements
    - service, device or user oriented

security concept at Uni Münster (4)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Virtualization
  - (hierarchical) interconnection and embedding of security functions wherever necessary requires many devices to be deployed
  - optimization concerning effort, flexibility and costs through intensive usage of virtualization technologies:
    - virtual LANs (vlans)
    - virtual routers (vrf)
    - virtual security functions (firewall, ips, ...)
    - virtual multiple VPN access
  - high performant devices centrally installed providing many virtual instances simultaneously

security concept at Uni Münster (5)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- User Self Care mechanism ("Mandantenfähigkeit")
  - development, implementation and maintenance of typically complex (security) configurations of many (security) instances difficult for staff of central network administration
  - local administrators of decentral *Net Areas* are much deeper involved in their configuration requirements
  - solution: management platforms should support authenticated and authorized access of local administrators to only their (virtual) instances of their *Net Area(s)*
    - relief of central administration
    - shorter delays, just in time
  - important: central administrators keep "master" control and can enforce default or mandatory settings

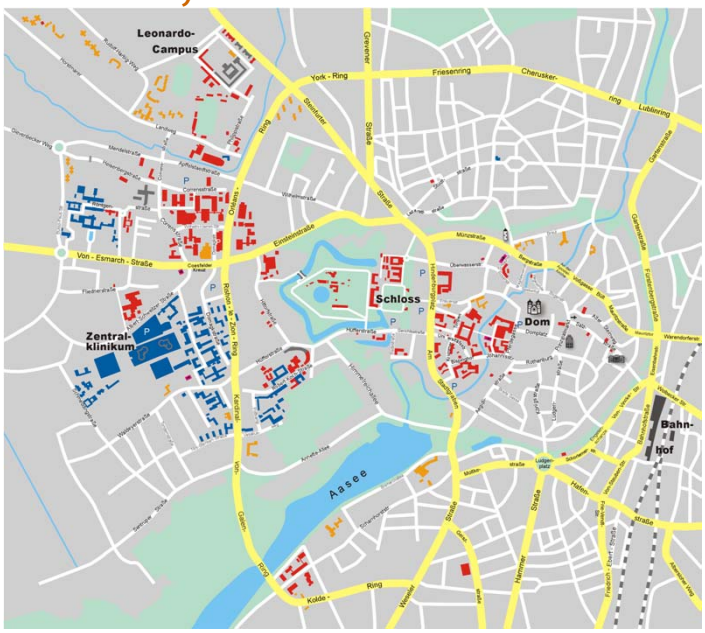
summarization

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- concept of *Net Areas* in *Structured Networks* enables
  - more simple and clear security rule sets
  - obvious and distributed responsibilities
  - delegation of administration to users (*user self care*)
- handling of (complex) security infrastructures also in larger enterprises does more scale and becomes more economic

University of Münster

ZENTRUM FÜR INFORMATIONS VERARBEITUNG



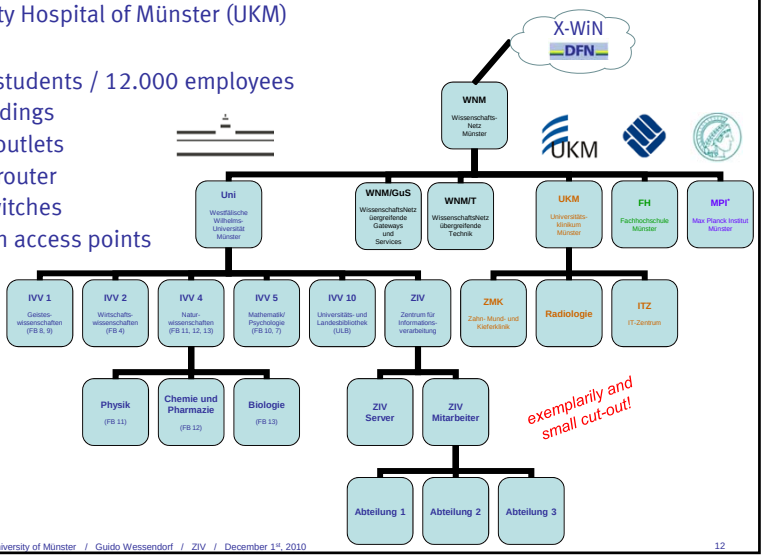
Map covers around 3.8 x 3.8 kilometers

= University
= UKM (clinics)

University of Münster

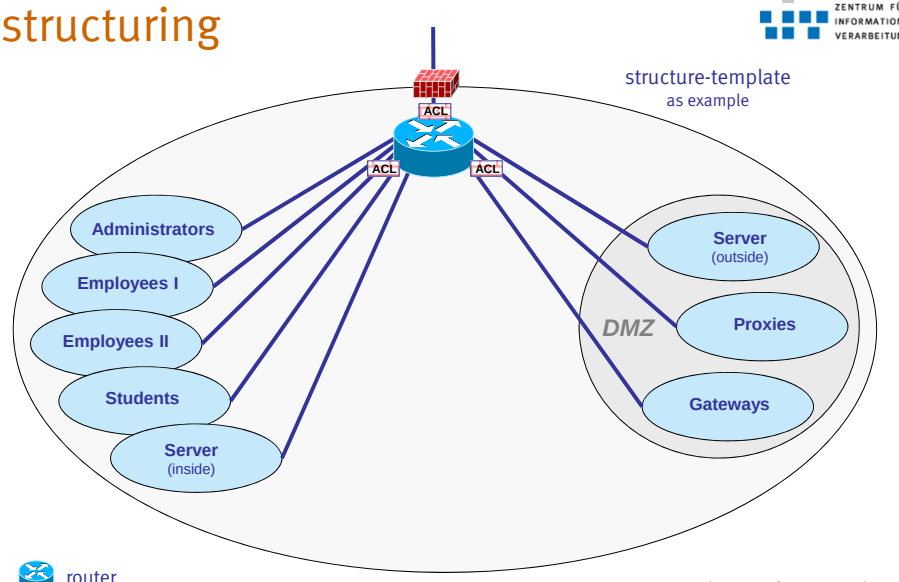
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- one network
  - University of Münster (WWU)
  - University Hospital of Münster (UKM)
- together
  - 36.000 students / 12.000 employees
  - 277 buildings
  - 46.451 outlets
  - 19 core router
  - 1701 switches
  - 911 wlan access points
- hierarchical organization



structuring

ZENTRUM FÜR INFORMATIONS VERARBEITUNG



router

group of *Net Areas* for (sub-)departments

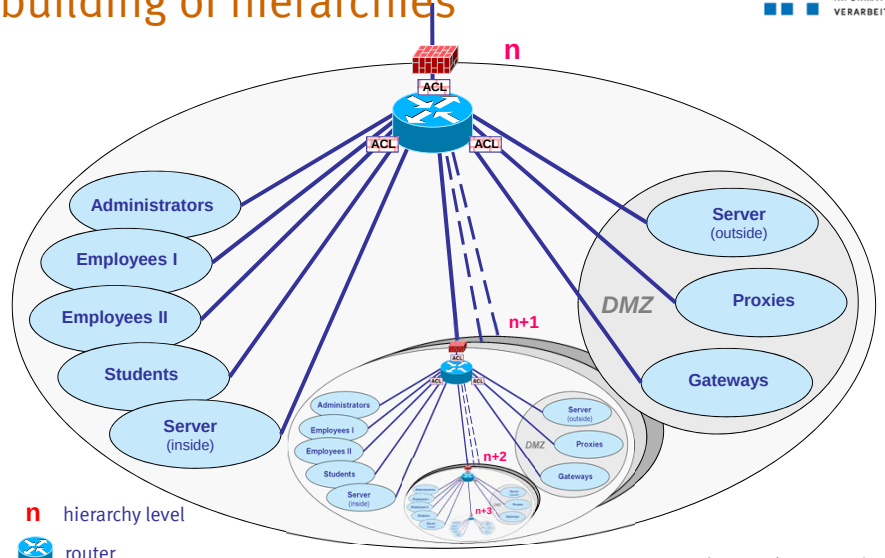
Net Area (vlan/subnet), collection of users/devices

ACL stateless packet screening

stateful inspection (firewall)

building of hierarchies

ZENTRUM FÜR INFORMATIONS VERARBEITUNG



n hierarchy level

router

group of *Net Areas* for (sub-)departments

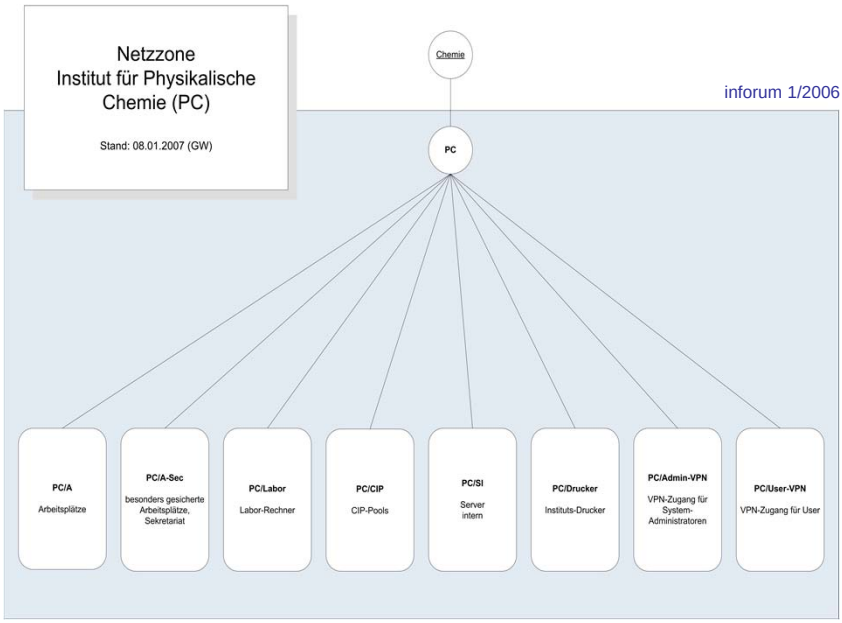
Net Area (vlan/subnet), collection of users/devices

ACL stateless packet screening

stateful inspection (firewall)

Institute of Physical Chemistry

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

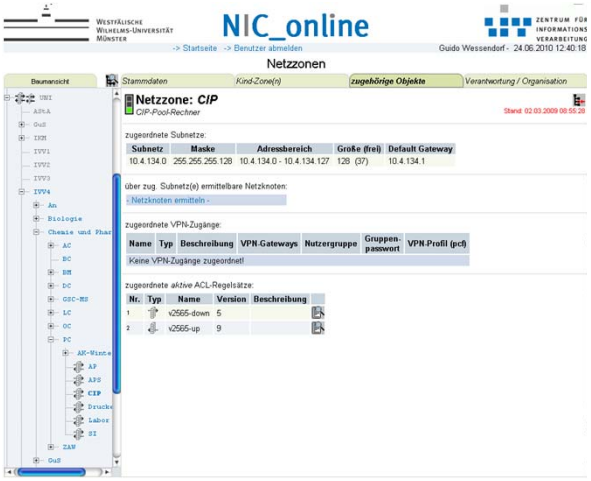


inforum 1/2006

Net Area management

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- self-development: *NIC_online*
- new: management of Net Areas included



VPN access

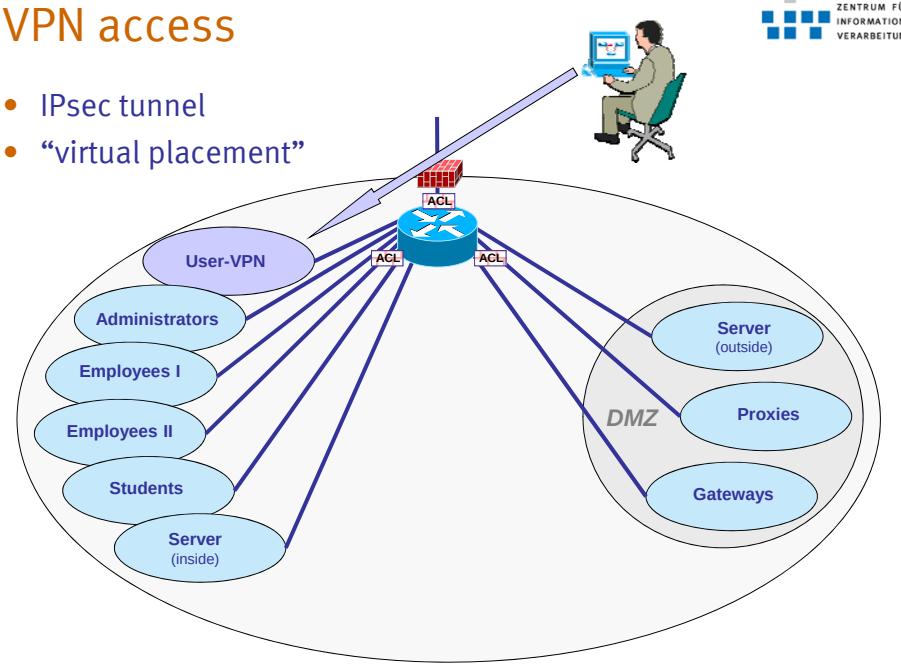
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- break through hierarchy to enable special or ad hoc access
- from somewhere
  - from other Net Areas
  - from Internet
- to somewhere
  - to other Net Areas or hierarchies
  - to Internet
- with differentiated authorization
  - e.g. `karl.maier@admin.math.uni-muenster.de`
- client-to-site or site-to-site

VPN access

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- IPsec tunnel
- "virtual placement"



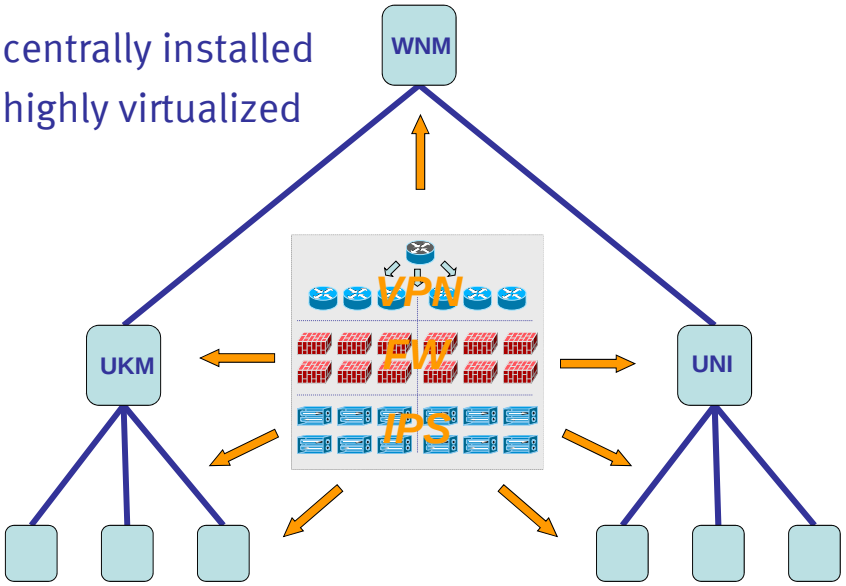
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

realization

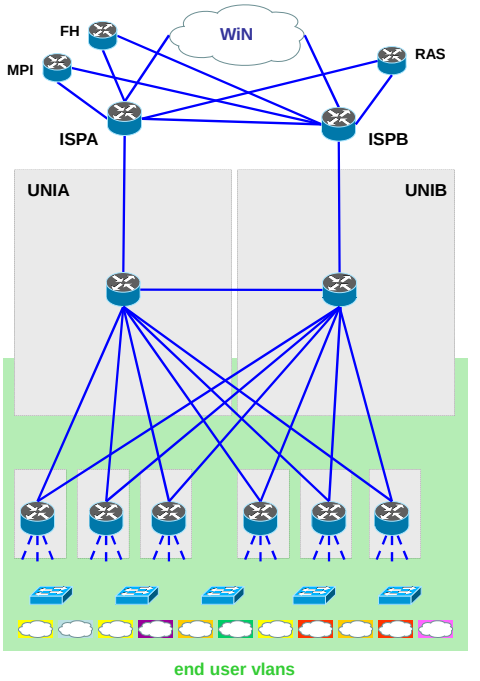
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

„new offer“: security services

- centrally installed
- highly virtualized



so far



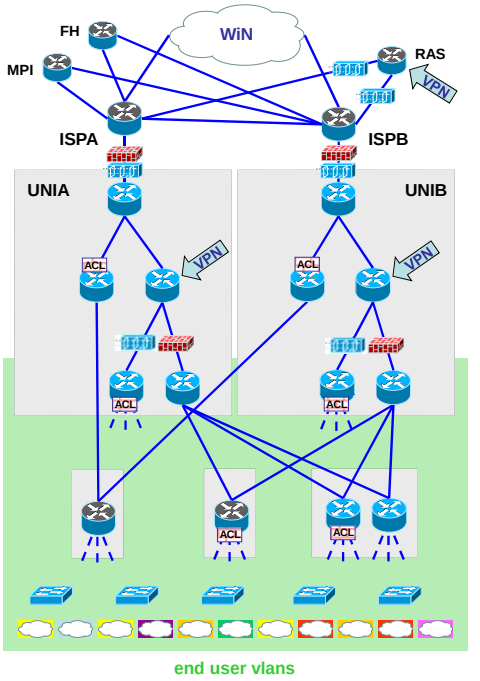
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

(exemplarily and incomplete)

router
chassis
virtual lan

Hints:
- L2 links not included
- L2 distribution area per vlan as small as possible
- UKM net similar to UNI

new



ZENTRUM FÜR INFORMATIONS VERARBEITUNG

(exemplarily and incomplete)

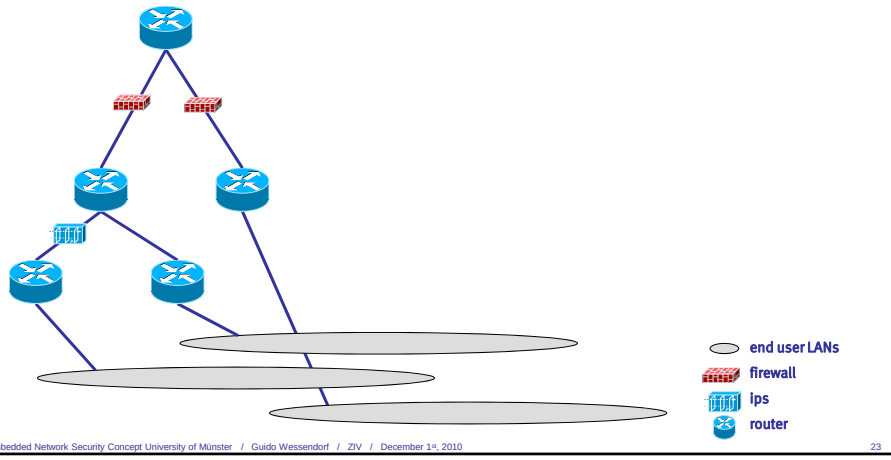
remote access
virtual ips
virtual fw
stateless packet screening
virtual router
router
chassis
virtual lan

Hints:
- L2 links not included
- L2 distribution area per vlan as small as possible
- UKM net similar to UNI
- not all L3 links included!

redundancy and load sharing

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

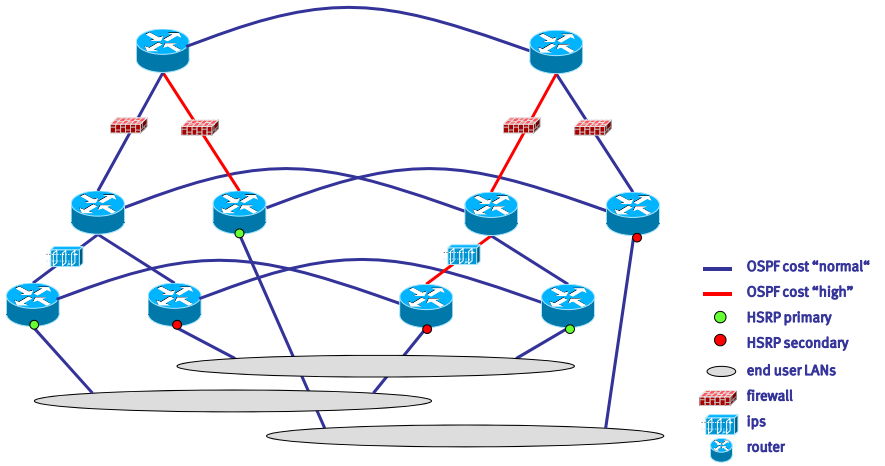
- for every part (routing, firewall, ips, ...)
- two redundant network trees
- no hot standby necessary (dynamic routing protocols)
- overbooking possible



redundancy and load sharing

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- for every part (routing, firewall, ips, ...)
- two redundant network trees
- no hot standby necessary (dynamic routing protocols)
- overbooking possible



Cisco Catalyst 6509

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Supervisor Engine 720 (3BXL)

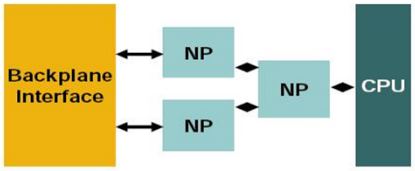
- 40 Gbps/slot (720 Gbps Crossbar)
- 4-port 10GE modules supported
- IPv4 routing in hardware, up to 400 Mpps
- IPv6 routing in hardware, up to 200 Mpps
- up to 1M routes (IPv4), 500k (IPv6)
- up to 1024 VRF (virtual router)
- 32k port ACLs (stateless, wire speed)

FWSM

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

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

RST-2504
9794_05_2004_c2

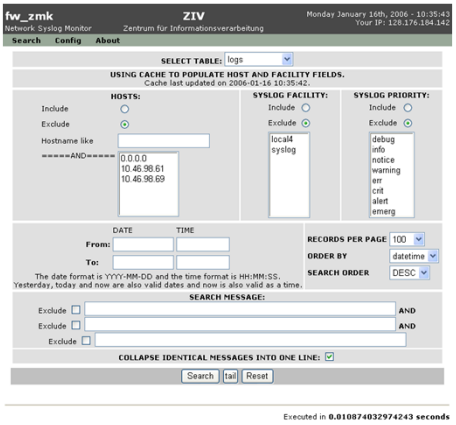
© 2004 Cisco Systems, Inc. All rights reserved.

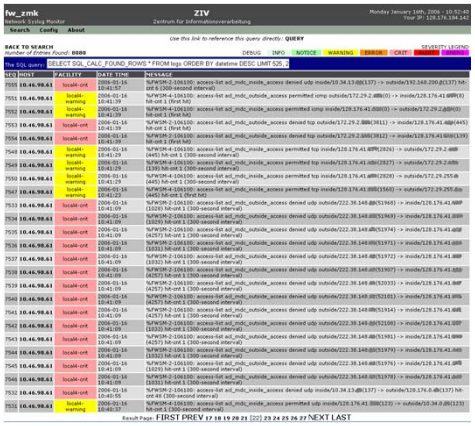
30

firewall management

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

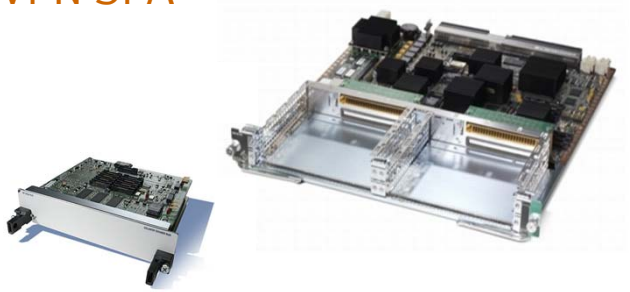
- Cisco Security Manager (CSM)
- syslog event management
  - open source implementation:
    syslog-ng + MySQL + Apache + php-syslog-ng





IPsec VPN SPA

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

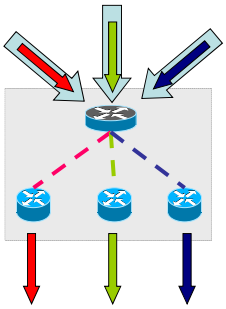


- shared port adapter (SPA) for carrier module for Catalyst
- 2.5 Gbps AES/3DES throughput
- up to 8.000 tunnels simultaneously
- tunnel setup rate 60 tunnels/sec
- up to 10 modules/chassis
- vrf support

IPsec VPN SPA

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- vrf support (vrf-aware-IPsec feature)



standard router
(VPN gateway addresses on loopback interfaces)

vrf routers

  - virtual tunnel end at arbitrary vrf (within same chassis)
  - complete routing integration (e.g. ospf)

McAfee IntruShield 4010

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- intrusion detection and prevention
  - signature based (e.g. anti virus)
  - behavior based (e.g. anti DoS)
  - known vulnerabilities
  - combined (day-zero-attacks)
- blocking in real time (if required)
- up to 2 Gbps throughput
- up to 1000 virtual systems (e.g. vlan based)
- transparent mode ("in-line mode")
- management front end multi-subscriber capable ("administrative domains")

prospects

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- further deployment of concept!
  - structuring
  - building of hierarchies
  - user self-care mechanisms (via network database “NIC_online”)
    - access and firewall rules management
    - port configurations
    - subscriber management
- end system security for VPN connections
  - policy enforcement
- content filtering / secure proxies
  - e.g.
    - WebSense
    - N2H2
    - WebWasher
    - BlueCoat
    - IronPort

inforum – information of University Münster Computing Centre (ZIV)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- inforum 1/2005
  - Netzseitige IT-Sicherheitsmaßnahmen des ZIV
    - http://www.uni-muenster.de/ZIV/inforum/2005-1/a17.html
- inforum 1/2006
  - Netzseitige IT-Sicherheitsmaßnahmen des ZIV 2006
    - http://www.uni-muenster.de/ZIV/inforum/2006-1/a04.html
  - Stateful-Firewall-Service des ZIV
    - http://www.uni-muenster.de/ZIV/inforum/2006-1/a06.html
  - VPN-Service des ZIV
    - http://www.uni-muenster.de/ZIV/inforum/2006-1/a05.html
- inforum 1/2007
  - Netzstrukturierung im Naturwissenschaftlichen Zentrum (NWZ)
    - http://www.uni-muenster.de/ZIV/inforum/2007-1/a20.html