1st esproject
Experience in Information Security Projects

Berlin, 23.-24. November 2010

Prof. Dr. -Ing. E. Eren
www.inf.fh-dortmund.de/eren
www.lisa-fh-dortmund.de

eren@fh-dortmund.de

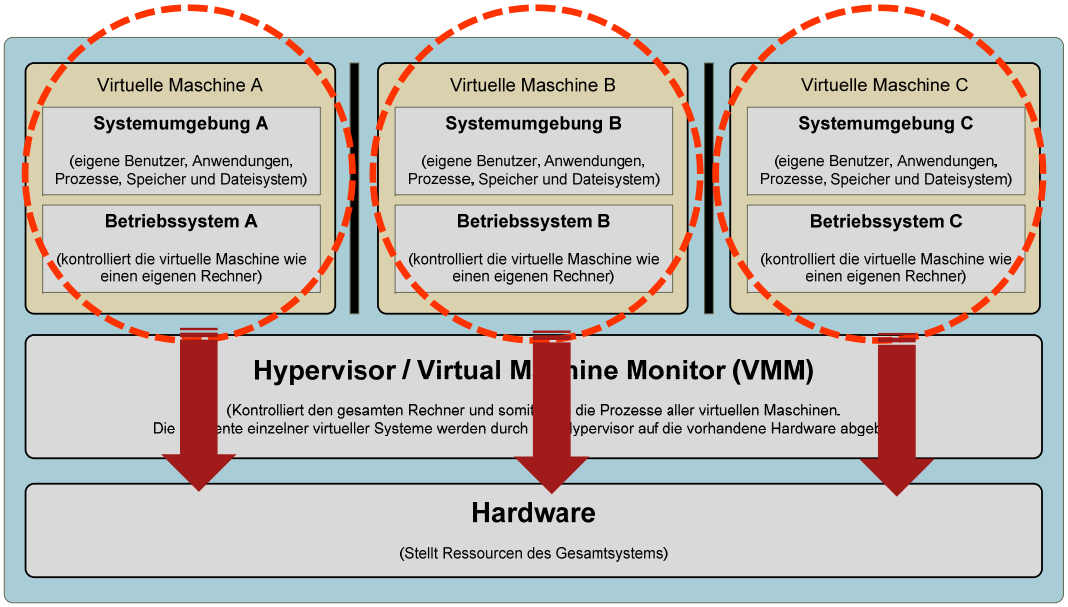
Hardwarebasierte Vollvirtualisierung

Virtualisierung

- Virtualisierung von Betriebssystemen ist seit geraumer Zeit etabliert.
- Doch mit Hilfe moderner Virtualisierungssoftware bestehen heute Möglichkeiten, sogar komplexe IT-Infrastrukturen und deren Komponenten zu virtualisieren:
  - Subnetze
  - Router
  - Switches
  - Firewalls
  - DMZ
  - etc.

Vollvirtualisierung

- Bei der Vollvirtualisierung (echte Virtualisierung) wird die Hardware des Hostsystems in mehrere VMs aufgeteilt.
- Die Gastsysteme innerhalb der VMs entsprechen weitestgehend der Architektur des Hostsystems und laufen getrennt voneinander – jeweils mit ihrem eigenen Betriebssystem.
- Jedem Gastsystem wird eine standardisierte Hardware bereitgestellt.
- Die VMs greifen nicht direkt auf die physikalische Hardware des Hosts zu.



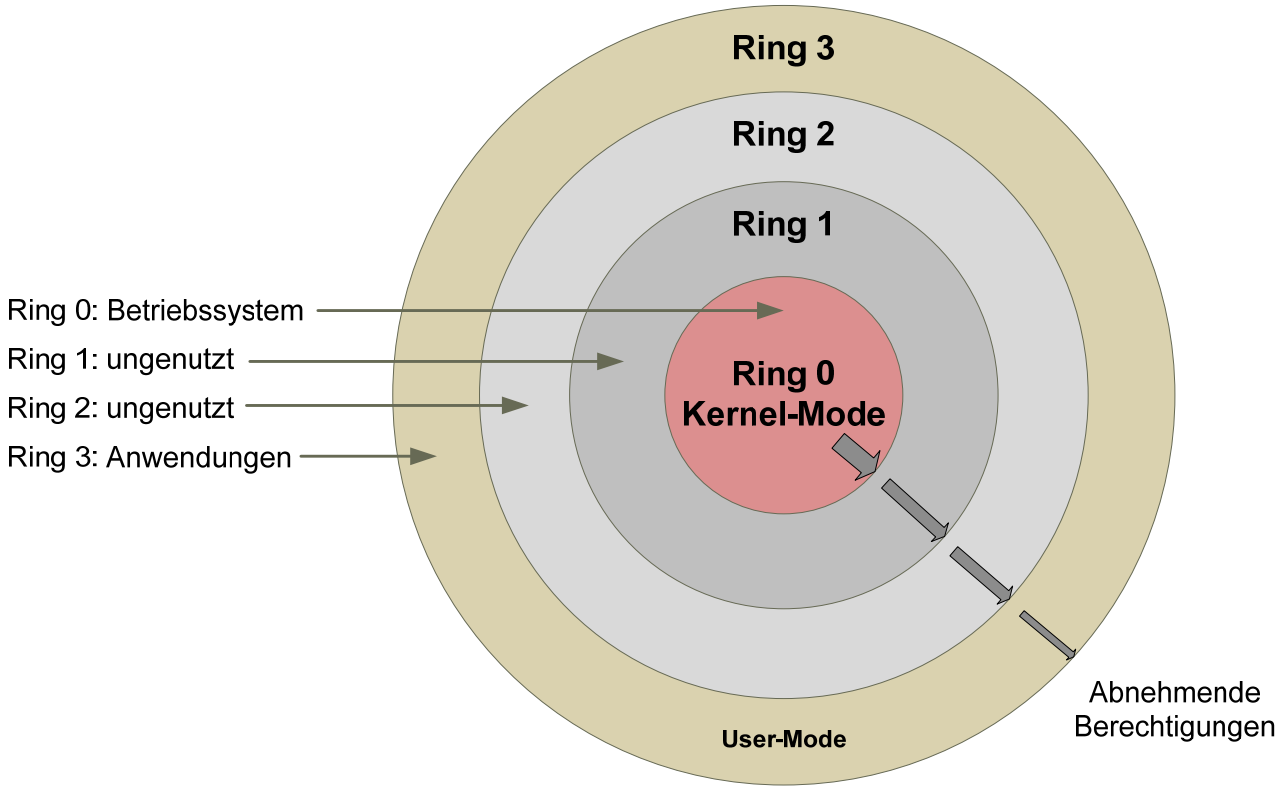
Hardwarebasierte Virtualisierung

- Hardwarebasierte Virtualisierung kombiniert Techniken der Voll- und Paravirtualisierung, wobei die Virtualisierungsfunktionalität in die Prozessorhardware integriert wird.
- Die Grundfunktionalität dieser Erweiterungen besteht in der Erkennung und gesonderten Behandlung von kritischen Operationen.
- Der allgemeine Trend zur Virtualisierung brachte Hardwarehersteller dazu, ihre neuen x86-Prozessoren um sog. Virtualisierungsfunktionen zu erweitern.
- Diese modernen Prozessoren unterstützen die Interaktion zwischen VMs und Hypervisor.

Hardwarebasierte Virtualisierung

- Hardwarebasierte Virtualisierung ist prinzipiell identisch zu Vollvirtualisierung.
  - Entscheidender Unterschied: Das Privilegiensystem der neuen Prozessoren ist erweitert.

Vollvirtualisierung



Klassisches Ring-Modell:

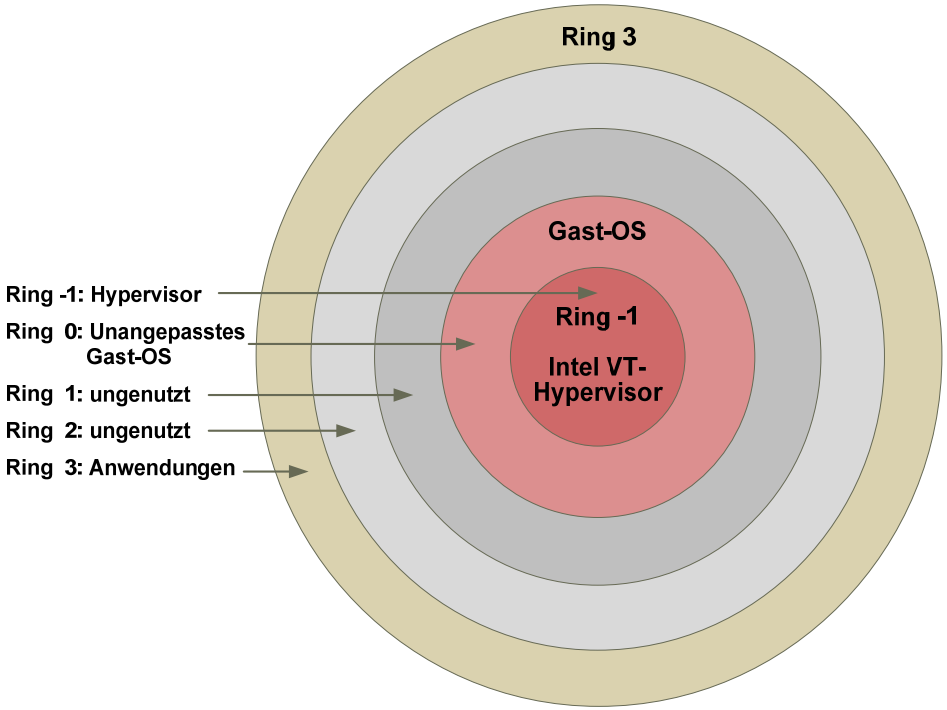
Das Betriebssystem läuft in Ring 0 und hat vollen Zugriff auf die Hardware. Es läuft im sog. Kernel-Mode.

Anwendungen laufen in Ring 3. Hierbei spricht man dann vom sog. „User-Mode“, der nur eingeschränkte Rechte besitzt und bspw. nur auf Speicherbereiche zugreifen darf, die der Anwendung vorher explizit zugewiesen wurden.

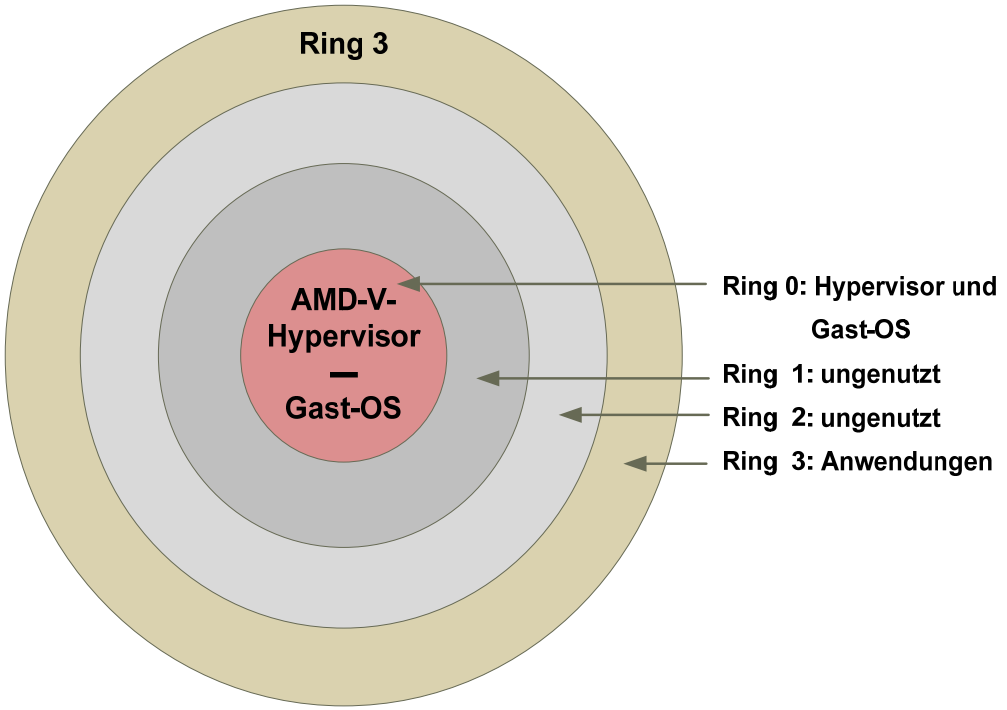
Zugriffsberechtigungen nehmen von Ring 0 nach 3 ab.

Ring 1 und 2 werden in modernen Betriebssystemen nur sehr selten genutzt.

Hardwarebasierte Virtualisierung



Ring-Modell bei Intel VT



Ring-Modell bei AMD-V

Hardwarebasierte Virtualisierung

- Gastbetriebssysteme
  - müssen nicht mehr in unprivilegierten Ringen betrieben werden, sondern deren Kernel kann direkt in Ring 0 laufen.
  - können somit unangepasst bleiben, da sie sich in ihrer gewohnten Umgebung befinden.
  - können den Prozessor direkt nutzen.

- Nach wie vor ist der Hypervisor für die Verwaltung und Kontrolle der VMs zuständig, verhält sich jedoch (im Gegensatz zur Vollvirtualisierung) rein passiv.

Hardwarebasierte Virtualisierung

- Durch die neuen zur Verfügung stehenden Befehlssätze können privilegierte Instruktionen regulär und somit sicher ablaufen.
- Ein Kontextwechsel zum Hypervisor ist nicht jedes Mal notwendig.
- Der Virtualisierungsprozess wird nicht gestört und damit der Virtualisierungsoverhead sehr stark reduziert.
- VMs laufen äußerst performant.

Hardwarebasierte Virtualisierung

Vorteile der hardwarebasierten Virtualisierung

- Geringer Virtualisierungs-Overhead
- Durch die Hardwareunterstützung sind die darauf aufbauenden Virtualisierungslösungen relativ schlank und es wird eine hohe Stabilität erreicht
- Gastsysteme müssen nicht angepasst werden (auch proprietäre Betriebssysteme können als VM installiert werden)
- Bessere Trennung der VMs auf Prozessorebene

KVM
(Kernel-based Virtual Machine)

KVM

- KVM ist eine Open Source Virtualisierungslösung (GPL) für Linux, welche Vollvirtualisierung auf x86-Hardware ermöglicht.
- KVM wurde 2006 von der israelischen Firma Qumranet veröffentlicht und wurde bereits ein halbes Jahr später in den Linux-Kernel (> 2.6.20) aufgenommen. Qumranet wurde im September 2008 von Red Hat gekauft.

- Seit der Linux-Version 2.6.20 ist KVM fester Bestandteil des Mainstream Linux-Kernels und ist inzwischen in den meisten Distributionen als Standardvirtualiserungslösung integriert.
- Auch in der Industrie erfährt KVM eine breite Unterstützung:
  - AMD, IBM, Intel, Suse und RedHat arbeiten bei der Weiterentwicklung zusammen.

KVM

- KVM ist eine Abspaltung vom Emulator QEMU, der verschiedene Prozessorarchitekturen wie PowerPC, ARM, Alpha, m68k, MIPS und Sparc emulieren kann.
- KVM stellt VMs die virtuelle Hardware (z.B. virtuelle Netzwerkinterfaces) zur Verfügung.
- KVM nutzt die Befehlssatzerweiterungen der neueren Intel- und AMD-Prozessoren (Intel VT und AMD-V).
- KVM bietet Unterstützung für paravirtualisierte Gerätetreiber für Netzwerk- und Blockgeräte (Massenspeicher). Hierdurch können die performancekritischen I/O-Zugriffe weiter optimiert werden. Hierbei baut KVM auf dem offenen Standard VirtIO auf.

- Gastsysteme laufen nahezu mit nativer Geschwindigkeit.
- CPU-Instruktionen werden direkt auf der Hardware des Hostsystems ausgeführt.

KVM

- Für die Netzwerkanbindung der VMs als auch die Verbindung untereinander bietet KVM mehrere Netzwerkoptionen:
  - Eine vollständige TCP/IP-Anbindung wird meist auf Basis von TUN/TAP-Interfaces realisiert.
  - Diese virtuellen Netzwerk-Kerneltreiber simulieren Netzwerkgeräte:
    - TUN simuliert ein Point-to-Point-Netzwerkgerät
    - TAP stellt ein Ethernet-Gerät dar.
- Ein virtuelles Netzwerkinterface einer VM wird mit einem TAP-Interface im Hostsystem gekoppelt, sodass dieses über eine Netzwerk-Bridge des Hostsystems verbunden und wiederum mit einer physikalischen Netzwerkschnittstelle werden kann.

KVM

Steckbrief KVM

Produkt	KVM
Hersteller	Qumranet, Inc. RedHat
Website	http://www.linux-kvm.org/page/Main_Page
Preis	Kostenlos (GNU General Public License)
Host-Plattform	Linux
Gäste	x86, x86_64, Linux, Windows, Haiku OS, AROS, ReactOS, FreeDOS, Solaris, BSD-Derivate
Merkmale	Hypervisor-System für Virtualisierungs-CPUs (Intel VT, AMD-V)

Vergleich der Virtualisierungslösungen

Lösung	Hostsystem	Hostplattform	Gastsysteme
Xen 3.2.0	Linux, openSolaris, NetBSD	x86, x86_64	Linux, NetBSD, Solaris, Windows (nur mit VT-x)
VMware Server 2.0 RC 1	Windows, Linux	x86, x86_64	Windows, Linux, BSD, Netware, Solaris, u.a.
VMware ESX 3.5 und ESXi 3.5	Eigenes Betriebssystem	x86, x86_64	Windows, Linux, Netware, Solaris, u.a.
Parallels Server / Server for Mac 3.0	Windows, Linux, OS X	x86_64	OS/2, Linux, Windows, BSD, u.a.
Microsoft Virtual Server 2005 R2 SP1	Windows Server 2003	x86_64	Windows, Linux
Microsoft Hyper-V	Windows Server 2008 (64-Bit)	x86_64	Windows ab 2000 SP4, Linux 2.4, BSD, Solaris
UML (Linux 2.6.25)	Linux 2.2 ab 2.2.15, 2.4, 2.6	x86, x86_64	Linux 2.4 (mit Patch), Linux 2.6
KVM	Linux ab 2.4	x86, x86_64	Linux, Windows, OS, ReactOS, FreeDOS, Solaris, BSD-Derivate, u.a.

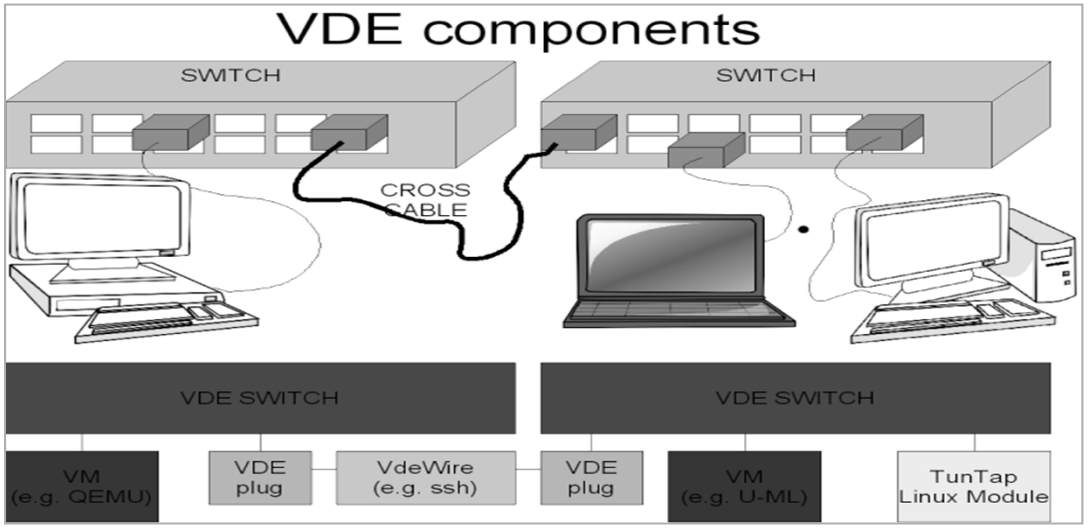
VDE
(Virtual Distributed Ethernet)

VDE

- Die Software VDE ist als weitere Netzwerkoption zu sehen.
- VDE ist Ethernet-konform und stellt virtuellen Infrastrukturen virtuelle Switches und virtuelle Kabel zur Verfügung.
- VDE-Netzwerke bestehen aus den Hauptkomponenten
  - VDE-*Switch*
  - VDE-*Plug*
  - VDE-*Wire*
  - VDE-*Cable*
- Sie stellen die Basis zum Aufbau von VDE-Netzwerken dar.

VDE

- VDE-Switches lassen sich durch VDE-Cables miteinander verbinden.
- TUN/TAP-Interfaces können an ein VDE-Switch angeschlossen sein. So lässt sich das virtuelle Netzwerk mit dem realen Netzwerk des Hostsystems verbinden.



- VDE-Wire lässt sich auch über Netzwerkprotokolle (z.B. netcat oder ssh) realisieren, sodass Verbindungen zwischen VDE-Switches auch über physikalische Netzwerke hergestellt werden können (z.B. virtuelle Netzwerke über einen SSH-Tunnel verbinden oder VPNs realisieren).

VDE

- KVM-VMs können über VDE-Netze direkt verbunden werden.
- VDE unterstützt auch VLANs nach IEEE 802.1Q.
- VMs verschiedener Virtualisierungslösungen, Emulatoren, reale Systeme (Betriebssysteme und Netzwerke) lassen sich miteinander verbinden.
- Auf Basis von VDE lassen sich einfach und flexibel virtuelle Netzwerke erstellen und Teilbereiche solcher Netze lassen sich sogar auf mehrere physikalische Rechner verteilen.

Vyatta

Vyatta

- Wie in der realen Welt sind Router und Firewalls auch in virtuellen Netzwerken wichtige Hauptkomponenten einer IT-Infrastruktur.
- Mittels Virtualisierungssoftware können virtuelle Router und Firewalls in Form von entsprechend konfigurierten VMs realisiert werden.

- Vyatta ist eine umfangreiche „Open-Source“ Router- und Firewall-Distribution auf Basis eines angepassten Debian Linux-Systems.
- Die Software wird von der kalifornischen Firma Vyatta Inc. unter der GNU General Public License (GPL) veröffentlicht.

- Weiterhin werden auch vorkonfigurierte Hardware-Router (sog. Hardware-Appliances) auf Basis von Vyatta angeboten.

Vyatta

- Vyatta bietet zahlreiche Netzwerkfunktionen, welche auch auf professionellen Hardware-Routern eingesetzt werden. Es werden diverse Routingprotokolle wie OSPF, BGP und RIP unterstützt.

- Jedoch bietet die Distribution nicht nur Routingfunktionen.
- Weitere Einsatzmöglichkeiten sind z.B.:

DHCP
NAT
PPPoE
VoIP QoS
WAN link load balancing
Site-to-Site Ipsec-VPN
SSL-based OpenVPN
RADIUS authentication
802.1q VLANs
Stateful Firewall
SNMP
IDS/IPS
Anti-Virus

Vyatta

- Konfiguration über das CLI:

Anzeigen der konfigurierten Netzwerkschnittstellen (*Operational Mode*):

```
vyatta@rt-ext~$ show interfaces
Interface     IP Address          State       Link    Description
eth0          172.22.136.168/20   up          up      WAN
eth1          192.168.0.1/24      up          up      LAN
eth2          192.168.4.1/24      up          up      VPN-DMZ
lo            127.0.0.1/8         up          up
lo            ::1/128             up          up
```

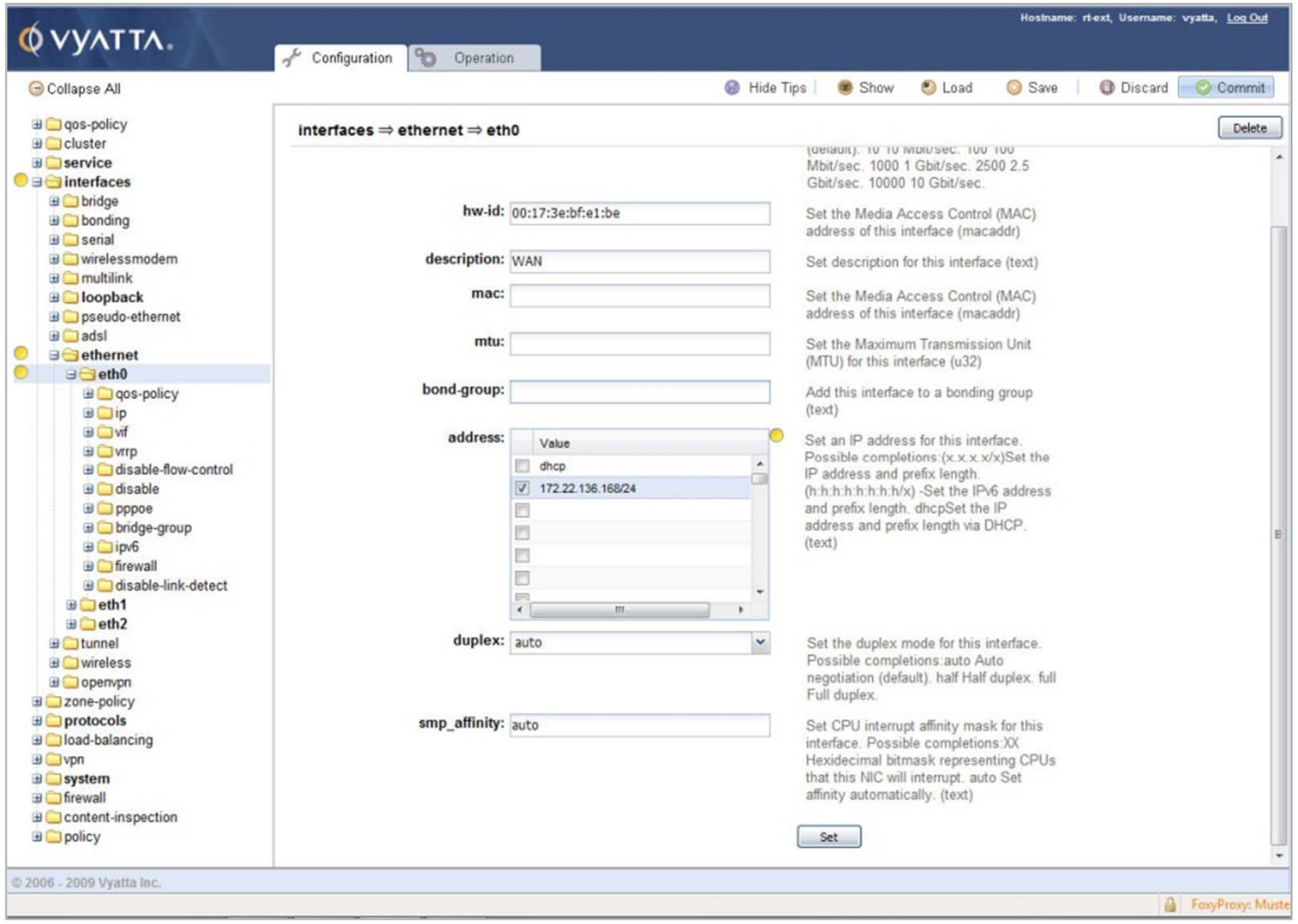
Setzen eines Name-Servers:

```
vyatta@rt-ext# set system name-server 172.22.1.10
```

Definition einer Port-Weiterleitung (*Destination*-NAT am Beispiel PPTP-Dienst):

```
vyatta@rt-ext# set service nat rule 100 destination port 1723
vyatta@rt-ext# set service nat rule 100 protocol tcp
vyatta@rt-ext# set service nat rule 100 inside-address address
192.168.4.10
vyatta@rt-ext# set service nat rule 100 type destination
```

Vyatta


VYATTA.
Hostname: rt-ext, Username: vyatta, Log Out
Configuration
Operation
Collapse All
Hide Tips
Show
Load
Save
Discard
Commit
qos-policy
cluster
service
interfaces
bridge
bonding
serial
wirelessmodem
multilink
loopback
pseudo-ethernet
adsl
ethernet
eth0
qos-policy
ip
vif
vrrp
disable-flow-control
disable
pppoe
bridge-group
ipv6
firewall
disable-link-detect
eth1
eth2
tunnel
wireless
openvpn
zone-policy
protocols
load-balancing
vpn
system
firewall
content-inspection
policy
interfaces ⇒ ethernet ⇒ eth0
Delete
Mbit/sec. 1000 1 Gbit/sec. 2500 2.5 Gbit/sec. 10000 10 Gbit/sec.
hw-id: 00:17:3e:bf:e1:be
Set the Media Access Control (MAC) address of this interface (macaddr)
description: WAN
Set description for this interface (text)
mac:
Set the Media Access Control (MAC) address of this interface (macaddr)
mtu:
Set the Maximum Transmission Unit (MTU) for this interface (u32)
bond-group:
Add this interface to a bonding group (text)
address:
Value
dhcp
172.22.136.168/24
Set an IP address for this interface. Possible completions:(x.x.x.x/x)Set the IP address and prefix length. (h:h:h:h:h:h:h:h/x) -Set the IPv6 address and prefix length. dhcpSet the IP address and prefix length via DHCP. (text)
duplex: auto
Set the duplex mode for this interface. Possible completions:auto Auto negotiation (default). half Half duplex. full Full duplex.
smp_affinity: auto
Set CPU interrupt affinity mask for this interface. Possible completions:XX Hexidecimal bitmask representing CPUs that this NIC will interrupt. auto Set affinity automatically. (text)
Set
© 2006 - 2009 Vyatta Inc.
FoxyProxy: Muste

Vyatta

- Vyatta ist eine leistungsfähige und interessante Alternative zu Hardware-Routern wie denen von Cisco oder Juniper.
- Vyatta wurde mit der Zielsetzung entwickelt, alle wesentlichen Merkmale moderner Hardware-Router abzubilden, welches auf gängiger x86-Hardware läuft.
- Dies impliziert enorme Vorteile in Bezug auf Kosten und Flexibilität.
- Durch den Einsatz moderner x86-Hardware erwies sich Vyatta auch in unabhängigen Vergleichstests in Bezug auf Durchsatz u. Performance als äußerst leistungsstark:
  - Im konkreten Vergleich mit Cisco-Routern wie Cisco 2821 und 7204VXR ergaben sich sogar deutlich bessere Leistungen.

LISA
(Laboratory for IT-Security Architectures)

LISA

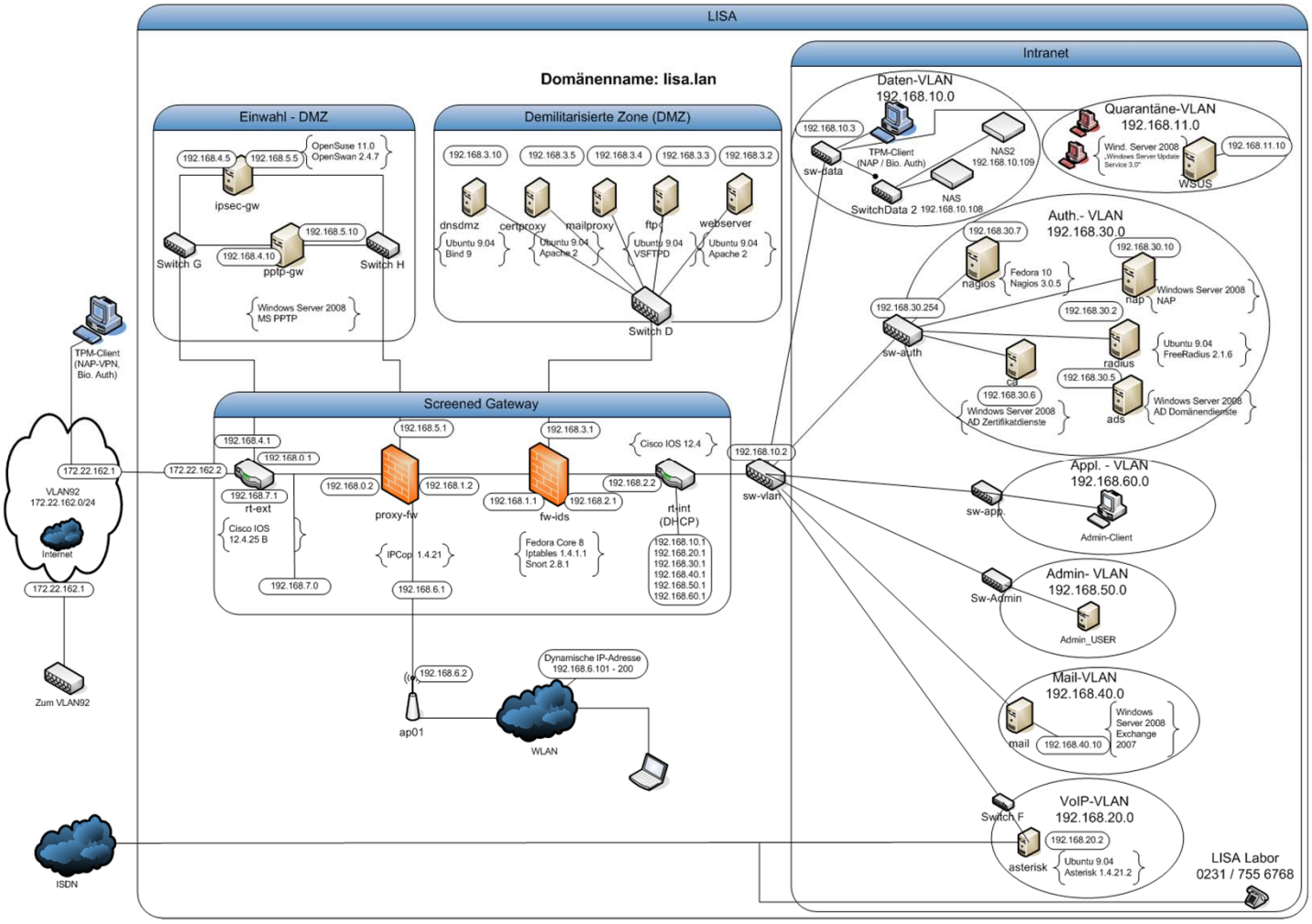
Laboratory for IT-Security Architectures

- Das „Laboratory for IT-Security Architectures – LISA” im Fachbereich Informatik der FH-Dortmund stellt eine modulare Entwicklungs- und Evaluations-Plattform für IT-Sicherheitsarchitekturen zur Verfügung.
- Hier können Sicherheitsmodelle und -architekturen exemplarisch diskutiert, erprobt und validiert werden.
- LISA wird sowohl für die praxisorientierte Lehre und Forschung, als auch als Demo-Center für Unternehmen eingesetzt.
- Es werden insbesondere Sicherheitsprobleme und -architekturen von KMU adressiert.

LISA

Laboratory for IT-Security Architectures

Topologiebeispiel für ein KMU



Virtualisierung von IT-Sicherheitsinfrastrukturen für Unternehmensnetze

Firewalling/Intrusion Detection bzw. Prevention
- Proxy-Firewall (ipcop)
- Application Firewall (iptables)
- Intrusion Detection System (Snort)
- DMZ (Web, DNS-Proxy, Mail-Proxy, FTP)
- DMZ für VPN-Server
- Border Router (Vyatta)
- Interner Router und Paketfilter (Vyatta)

PKI
- Zertifikatsserver – Unternehmens-PKI
- Mail-Server (MS Exchange)

AAA
- RADIUS-Server
- Active Directory Server (ADS)

VPN
- PPTP-VPN-Server (Windows 2008/Monowall)
- IPSEC-VPN-Server (StrongSwan)

Trusted Computing
- NAP/NAC (Microsoft 2008 NAC Server)
- TNC-Server (freeRADIUS TNClib)

Voice-over-IP
- VoIP-Server (Asterisk)

Network Monitoring
- NAGIOS

VISA
(Virtual IT-Security Architectures)

Projekt VISA

- IT-Infrastrukturen sind mittlerweile auch schon in KMU komplex:
  - Rechner
    - Desktopcomputer,
    - Laptops,
    - Server, …
  - Peripherie (z.B. Multifunktionsdrucker)
  - Netzwerkkomponenten
    - Router,
    - Switches, …
  - Sicherheitskomponenten
    - Firewall,
    - Authentisierungsdienste,
    - Intrusion Detection, …

Projekt VISA

- Die Integration neuer Sicherheitskomponenten erfordert oft neue Hardware und den Umbau der Netztopologie, der ohne genaue Kenntnis der Auswirkung umgesetzt werden muss.
- Die Auswirkungen von Änderungen an solchen Infrastrukturen sind oft erst im Operativbetrieb zu erkennen.
- Da immer mehr KMUs ein profundes IT-Risikomanagement (Basel II, Conformance, Compliance) vorweisen müssen, muss nachweisbar sein, dass die IT-Infrastruktur über ausreichende Schutzmechanismen verfügt (Virenabwehr, Zugangssteuerung, Schutz von Daten über Zugriffsrechte, IT-Notfallplanung und -regelung).
- Absichern von Einzelkomponenten – insbesondere im Verbund mit anderen Komponenten im Sinne eines ISMS ist kein einfaches Unterfangen.

Projekt VISA

- KMUs können für das operative IT-Management wenig Ressourcen (Know-how=Personal + Hardware + Infrastruktur) vorhalten.
- Deshalb muss für KMUs der Umgang mit IT-Infrastrukturen vereinfacht werden.
- Dies ist möglich durch Einsatz von Virtualisierung und Simulation von IT-Infrastrukturen.

- Vor diesem Hintergrund wurde im Projekt VISA „VISA - Virtual IT-Security Architectures“ wurde auf Basis von „Open Source“-Lösungen eine komplexe IT-Sicherheitsinfrastruktur für mittelständische Unternehmen virtualisiert.
- Hierbei kamen zum Einsatz:
  - KVM als Hardwarebasierte Vollvirtualisierungslösung
  - VDE zum Aufbau von virtuellen Netzwerken
  - Vyatta als Router-Distribution

Virtual Security Appliances

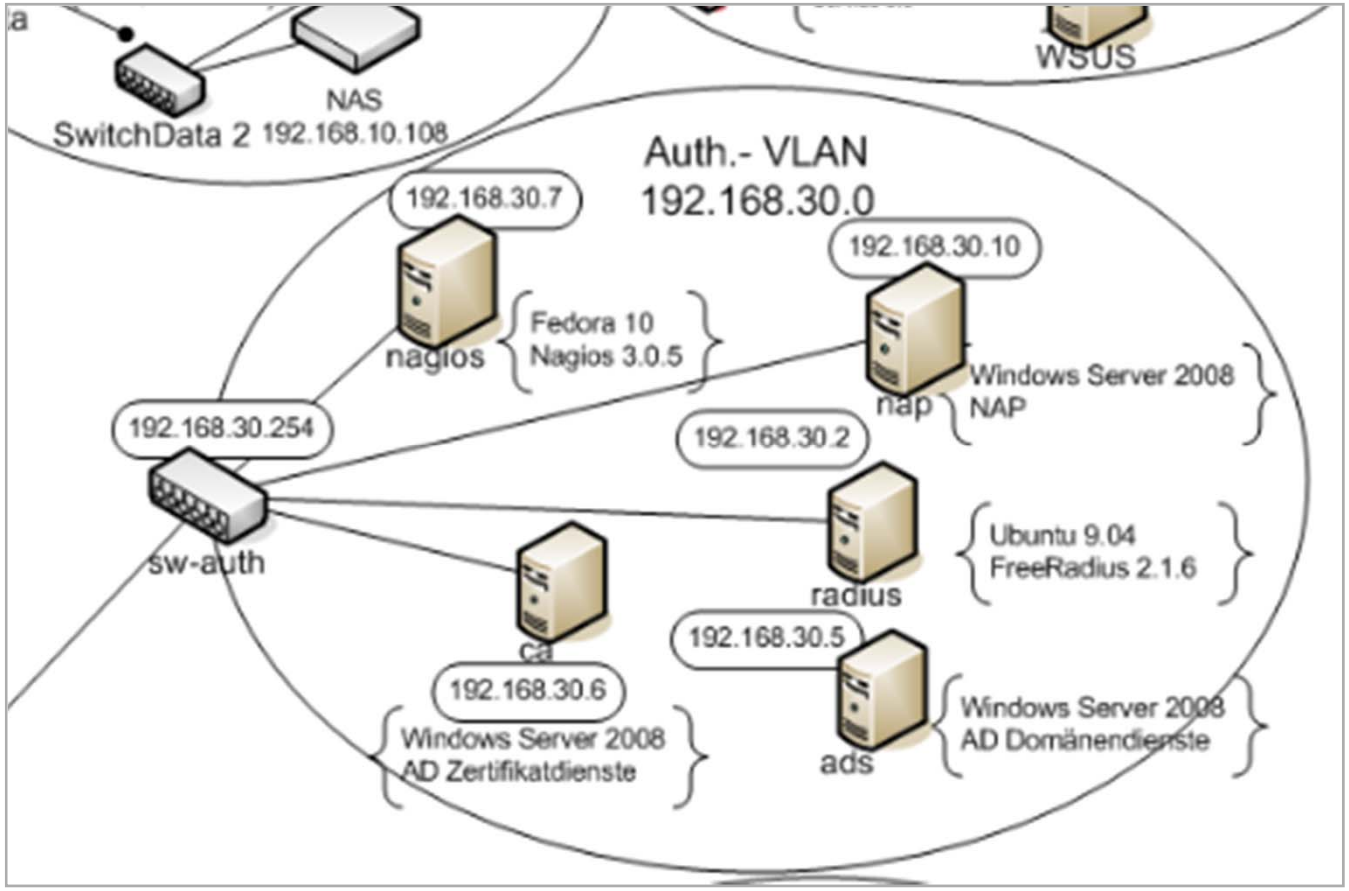
Virtual Security Applicances

- Durch Kombination dieser Technologien lassen sich komplexe IT-Infrastrukturen bis auf Layer 1 des ISO-OSI-Modells virtuell abbilden.

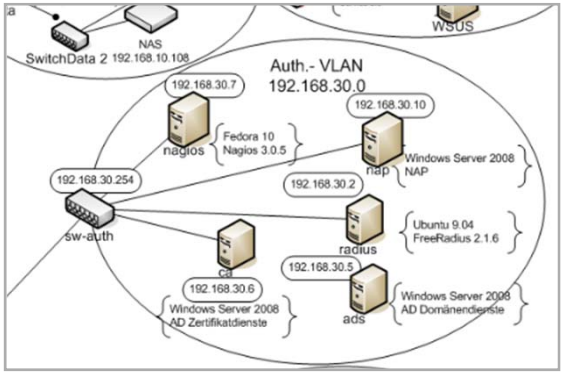
- Mit Hilfe von KVM, VDE und Vyatta lassen sich auch „Virtual Security Appliances“ modular und flexibel realisieren, die in die bestehende IT integriert werden können und somit diese erweitern und absichern.

LISA
Laboratory for IT-Security Architectures

Virtual Security Applicances



ESPI - Enterprise Security Plug-In



- RADIUS-Server (Authentisierung, Autorisierung, Accounting)
- Active Directory Server (ADS)
- Zertifikatsserver (CA/RA) – Unternehmens- PKI
- NAGIOS (Network & Infrastruktur Monitoring)

Unternehmens-IT

Vielen Dank