GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

# Virtualisierung ganzer Netzsegmente

*Prof. Dr.-Ing. Kai-Oliver Detken*

*DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen*

VISA

# Vorstellung der DECOIT GmbH


- Gründung am 01.01.2001 als reines Consulting-Unternehmen
- Fokus: Herstellerneutrale, ganzheitliche Beratung
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
- Seit 2002: Hinzunahmen des Systemmanagements, um Herstellerlösungen oder stabile Open-Source-Lösungen anzubieten
- Seit 2002: Hinzunahme der Software-Entwicklung, um Individuallösungen mit hohem Innovationscharakter entwickeln zu können oder Herstellerlösungen zu ergänzen
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen
- Aktueller Mitarbeiterstand: 15

# Dienstleistungen / Portfolio

- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von IT-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

**www.decoit.de**

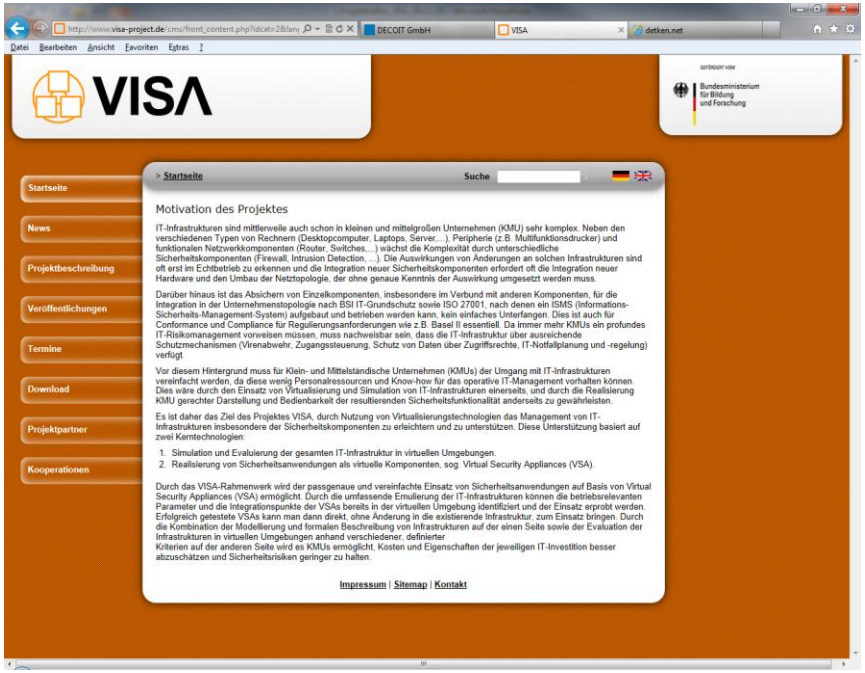
# Virtualisierung und Cloud Computing

- Für das Jahr 2012 stehen Cloud Computing, Mobile Applikationen und IT-Sicherheit ganz oben auf der Liste
- Leicht zurückgegangen ist die Virtualisierung
- Private-Clouds können als Virtualisierungs-lösung in jedem Fall dazugezählt werden

# Ausgangslage

- IT-Infrastrukturen sind mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) relativ komplex
- Die Auswirkungen von Änderungen sind oft erst im Realbetrieb zu erkennen
- Zusätzlich müssen auch BSI IT-Grundschutzanforderungen heute umgesetzt werden
- Die Virtualisierung hat zunehmend Einzug gehalten und wird die Komplexität noch erweitern
- Daher sollte der Umgang mit IT-Infrastrukturen vereinfacht werden, um
  - Konfigurationsfehler zu minimieren
  - Hohe Verfügbarkeit zu erreichen
- Um diese Problematik zu lösen wurde das Forschungsprojekt VISA (Virtual IT Security Architectures) ins leben gerufen

# VISA-Projekt

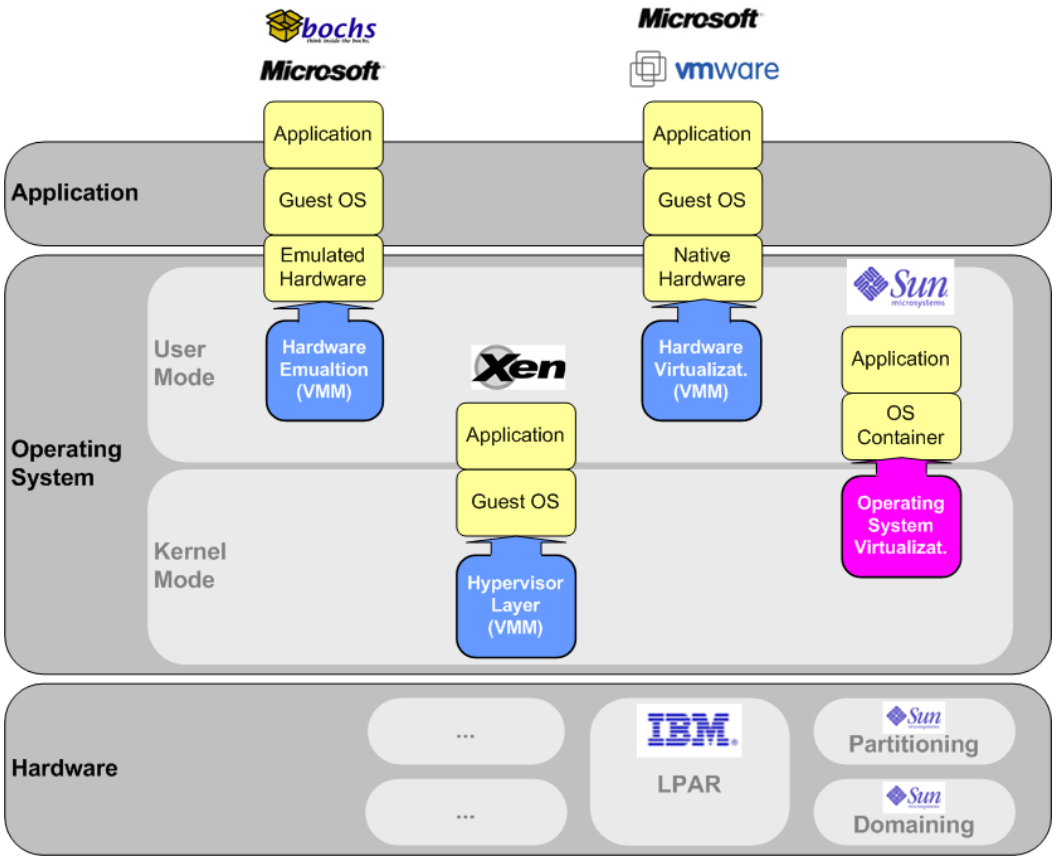



- Das VISA-Projekt ist ein nationales BMBF-Projekt
- Es startete am 01. August 2011 und wird im Juli 2013 enden
- Folgende Partner sind involviert:
  - DECOIT GmbH (Konsortialführer, Bremen)
  - Fraunhofer SIT (Darmstadt)
  - FH Dortmund (Dortmund)
  - Collax GmbH (Ismaning)
  - IT-Security@Work (Mainz)
  - NICTA (Sydney, Australien)
- Es gibt bereits Kooperationen mit anderen F&E-Projekten

# Ziele des VISA-Projektes

- VISA erstellt ein Framework, das das Erproben von VSAs in nachgebildeten, praxisorientierten Szenarien erlaubt. Hierfür sieht das Konsortium folgende technischen Herausforderungen bzw. Ziele:
  - Entwicklung und Packetierung verschiedener VSA-Module, die unterschiedliche Bereiche der IT-Sicherheit abdecken.
  - Eine automatisierte und dynamische Umgebung, die eine experimentelle Erprobung verschiedener Netztopologien und den Einsatz von VSAs erlaubt.
  - Modelle, die die Simulation der Netztopologien steuern.
  - Jede VSA muss am Ende als virtuelles Image vorliegen und durch das Deployment-System entsprechend dem zugrunde liegenden Modell konfiguriert werden können.
  - Es wird ein Modell bzw. Ausdruckssystem benötigt, um das Deployment zu steuern.
  - Eine Bibliothek von virtuellen Images wird benötigt, um die möglichen Wirkszenarien zu bauen.

# Virtualisierungslösungen



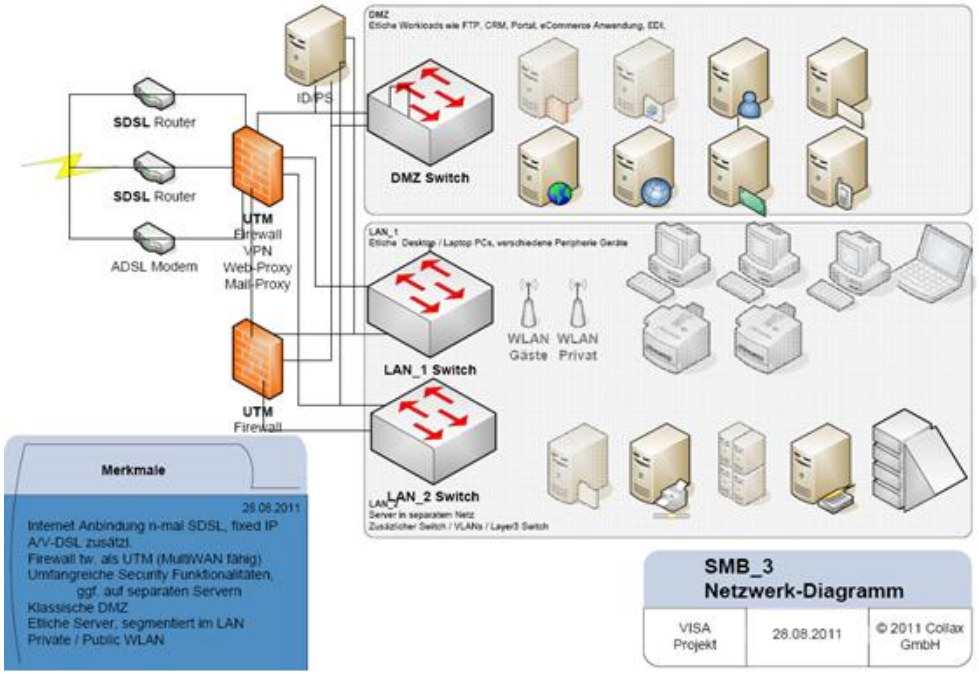

- Das VISA-Projekt hat sich auf KVM als Basis verständigt:
  - Einzige freie Lösung am Markt
  - Breite Unterstützung
  - Hohe Performance (Hardware-basiert)
  - Fester Bestandteil des Linux-Kernels
  - Keine Lizenzkosten (GNU GPL)

# Definition einer Virtual Security Appliance (VSA)

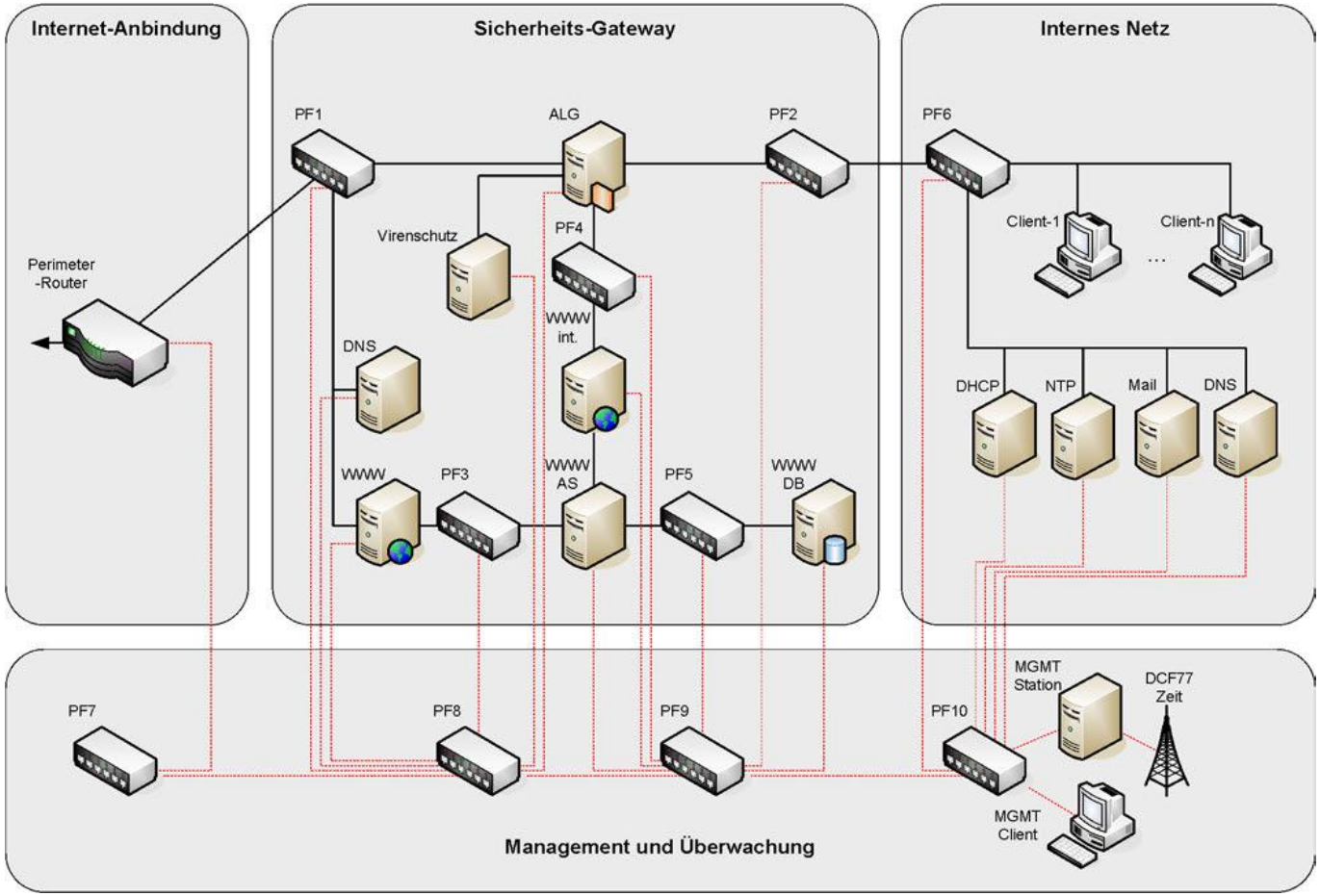
- **Virtual Appliance (VA):**
  - Als VA wird das Image einer Virtuellen Maschine (VM) bezeichnet, welches ein installiertes und vorkonfiguriertes Softwaresystem enthält
  - Hierbei beinhaltet dieses Image auch schon das Betriebssystem selbst.
- **Virtual Security Appliance (VSA):**
  - Als VSA werden verschiedene Virtual Appliances bezeichnet, die vorrangig der Sicherheit dienen
  - Von der Netzwerksicherheit (Layer 2) bis zur Anwendungssicherheit (Layer 7)
  - Mit Hilfe von VSAs wird versucht, IT-Hard- und Software zu virtualisieren

# Was soll abgebildet werden mit einer VSA?

- Die IT-Infrastruktur eines KMU
  - DMZ
  - Firewall
  - IDS
  - Switches
  - Remote-Zugänge
  - E-Mail-Server
  - FTP-Server
- Dazu wurden verschiedene KMU-Szenarien untersucht und beschrieben
- IT-Sicherheitsniveau und Verbesserungen durch die VSA wurden ebenfalls untersucht / beschrieben



# Grundarchitektur ISi-LANA nach BSI

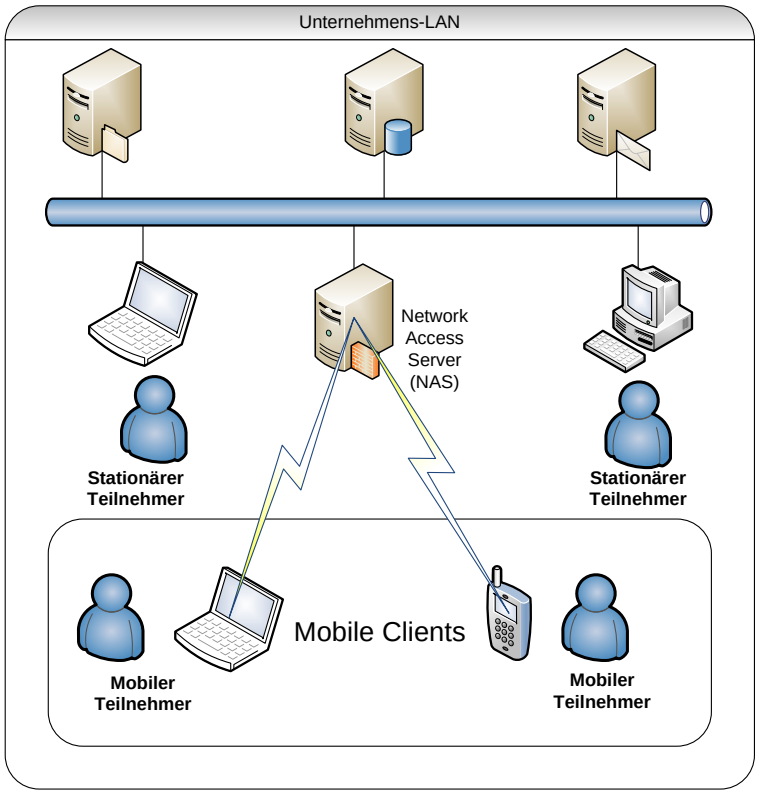



Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

# Was kann durch VSAs alles abgebildet werden?

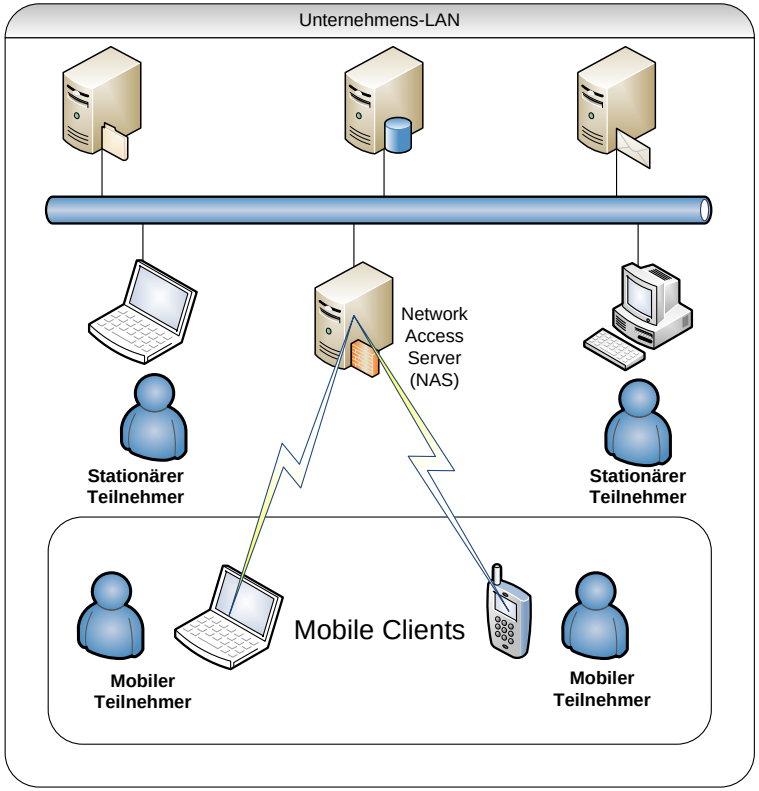
- Was sollten die VSA-Komponenten abbilden?
  - **Integrierbarkeit:** Komponente soll als autarke Einheit in bestehende Infrastrukturen integriert werden können
  - **Steuerbarkeit:** Überwachbarkeit einer VSA mittels GUI oder z.B. libvirt
  - **Modularität:** VSA sollte modular konzeptioniert sein, um eine flexible Anbindung ermöglichen zu können
  - **Vergleichbarkeit:** möglichst ohne Unterschiede zu physikalischen Derivaten
  - **Sicherheit:** Zugriffs- und Datensicherheit muss gewährleistet werden können
- Was sollten die VSA-Bereiche abbilden?
  - **Konfigurierbarkeit:** einfache Konfiguration und Verbreitung
  - **Sicherheit:** Absicherung eines gesamten VSA-Bereichs
  - **Autonomie/Adaptationsfähigkeit:** Integration in bestehende Infrastrukturen soll autonom ablaufen, um selten neue Konfigurationen durchführen zu müssen
  - **Verfügbarkeit/Migrierbarkeit:** Redundanz und schneller Wechsel auf unterschiedlichen Knoten zur Erhöhung der Verfügbarkeit

# Beispiel: VSA „Secure Remote Access” (1)



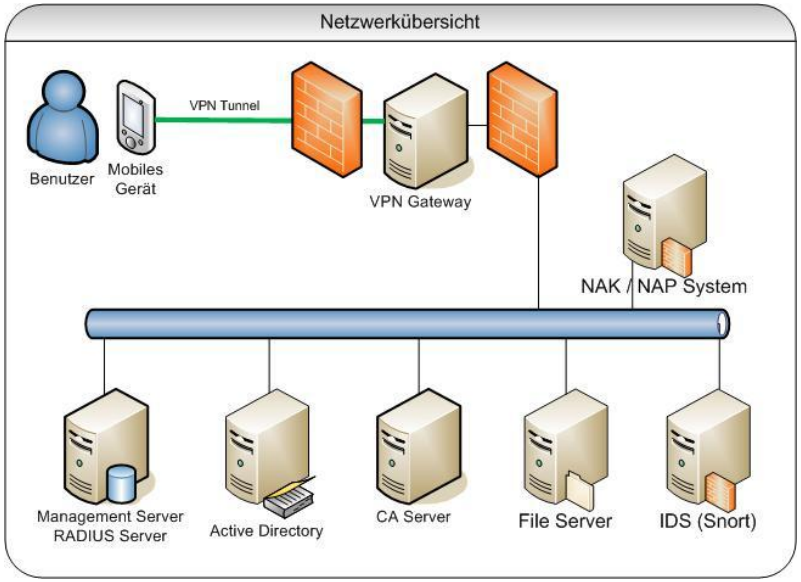

- **VPN-Gateway:** Teilnehmer authentifiziert sich über einen VPN-Zugang am VPN-Gateway. Damit ist der Teilnehmer bekannt, aber die Hardware stellt noch ein Sicherheitsrisiko dar.
- **TNC-Server:** Die vom TNC-Client erhaltenen Integritätsmessungen werden entgegengenommen. Anschließend fällt er anhand der Policy-Auswertung eine Entscheidung, ob der Zugriff des mobilen Endgeräts gestattet wird oder nicht.
- **TNC-Client:** Der Client bildet die Schnittstelle zwischen dem Network Access Requestor und den Plug-Ins des mobilen Endgeräts, welche die Informationen von Antivirus-Systemen oder anderen sicherheitsrelevanten Komponenten sammeln.

# Beispiel: VSA „Secure Remote Access” (2)



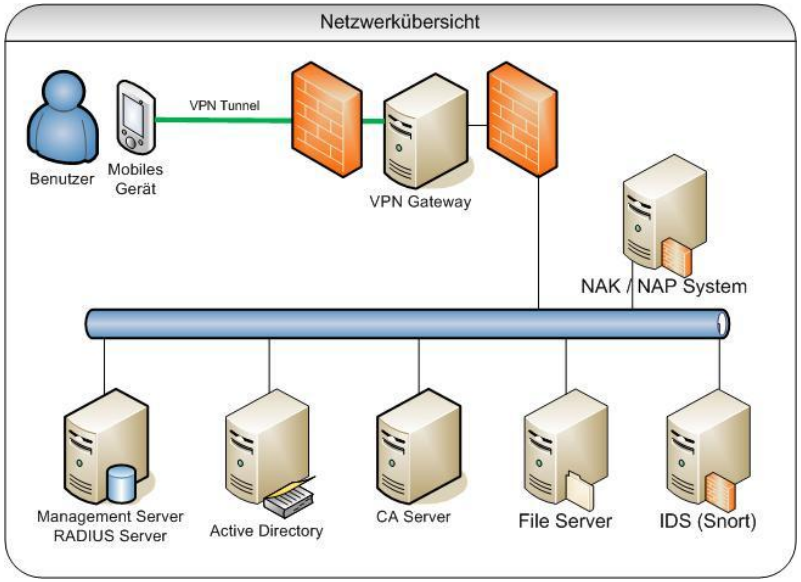

- **RADIUS:** enthält die Einwahlprofile und Konfiguration der Teilnehmer, die sich auf das Unternehmensnetz von außen verbinden dürfen. Eine Synchronisation mit dem internen Verzeichnisdienst wäre sinnvoll.
- **LDAP:** eine Authentifizierung über den Verzeichnisdienst LDAP kann vorgenommen werden. Außerdem wird angestrebt einen TNC-Server als VSA anzubieten sowie die Integration von TNC-Clients in anderen VSAs zu zeigen.
- **PKI-Server:** Bei Bedarf kann auch eine Zertifizierungsstelle (CA-Server) mit in das Szenario eingebunden werden, bei welcher bei Benutzeranlage durch das VPN-Management-System ein Zertifikat beantragt wird und für den Benutzer hinterlegt wird.

# Beispiel: VSA „Metadata Access Control” (1)




- **IF-MAP-Server:** Der IF-MAP-Server sammelt sämtliche Informationen der IF-MAP-Clients und konsolidiert diese zu einer gemeinsamen Datenbasis. Zustandsänderungen und Anomalien werden hier erkannt und an die relevanten Systeme weitergeleitet.
- **Firewall (iptables) IF-MAP-Client:** Auf Basis des IF-MAP-Protokolls wird eine VSA angestrebt, die eine dynamische Konfiguration einer Firewall, basierend auf dem Status des Gesamtnetzes, durchführt.
- **Android IF-MAP-Client:** Hier soll eine VSA angestrebt werden, die das Auswerten unterschiedlicher Eigenschaften ermöglicht. Dieses kann die IP-Adresse, MAC, OS-Version, installierte Anwendungen inkl. Berechtigungen, sowie die Position eines Endgerätes sein.

# Beispiel: VSA „Metadata Access Control” (2)




- **Snort IF-MAP-Client:** es wird die Aufbereitung und Veröffentlichung von Snort-Meldungen vorgenommen. Dies könnte verdächtiger Datenverkehr oder eine Portscan-Erkennung sein. Snort kann auch als unabhängige VSA gesehen werden, die in mehreren Instanzen eingesetzt werden kann.
- **RADIUS-IF-MAP-Client:** ermöglicht das Auslesen und Veröffentlichen von RADIUS-Informationen (auch Anmeldung und Abmeldung eines Clients). Bei einem Scheitern der Authentifizierung, wird diese Information an die Gateway-VSA senden. Somit kann die Gateway-VSA den weiteren Datenverkehr unterbinden.
- **DHCP IF-MAP-Client:** Dieser Netzwerkdienst zur automatischen Verteilung von IP-Adressen kann ebenfalls IF-MAP-fähig gemacht werden und so Einfluss auf die Netzwerkdienste geltend machen.

# Verbesserungsmöglichkeiten durch VSAs

- Die gesamte sicherheitsrelevante IT-Infrastruktur könnte durch VISA virtuell konzipiert und getestet werden
- Anschließend könnte man, nach erfolgreichen Tests, die Konfiguration oder die gesamte virtuelle Umgebung übernehmen
- Alle Dienste und Server könnten redundant ausgelegt werden, um eine 100%ige Verfügbarkeit zu erhalten
- Die komplette IT-Infrastruktur könnte komplett virtuell vorgehalten werden. Dadurch lassen sich auch Redundanzen (wie Firewall oder Router) einfacher aufbauen, um neben der IT-Sicherheit auch die Verfügbarkeit zu gewährleisten
- Die in VISA entstehenden Werkzeuge zum Management mehrerer VSAs entfalten in Umgebungen dieser Größe erstmals einen Nutzen, weil sie zur Vereinfachung, besseren Überwachungen und effizienterem Betrieb beitragen
- Durch die Flexibilisierung der Infrastruktur bei gleichzeitiger Komplexitätsreduktion bleibt für die IT-Mitarbeiter mehr Zeit, um sich dem Thema IT-Sicherheit pro-aktiv zuwenden zu können, sowohl bzgl. Know-how-Aufbau als auch operativer Umsetzung

# Aussichten

- Das VISA-Projekt geht jetzt in die Entwicklungsphase
- Dabei stehen folgende Aspekte im Vordergrund:
  - VSA-Umsetzung (u.a. SRA-VSA und MAC-VSA)
  - Management von VSAs
  - Verbreitung (Deployment) der VSAs
  - Schaffung virtuelle Switch-/Router-Umgebungen
  - Schnittstellenformate
  - Testtools
- Die Modellierung von Sicherheitsaspekten und -maßnahmen wird parallel zur Entwicklung untersucht werden

# Vielen Dank

***Besuchen Sie uns auf der CeBIT:***

***DECOIT GmbH: Halle 2, Stand D48***

VISA

# Copyright 2011-2013

*Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1160“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.*