GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Kooperationstreffen

in Frankfurt (Oder) bei der IHP GmbH

Prof. Dr.-Ing. Kai-Oliver Detken

VISA

Agenda

- 13:00 Uhr Vorstellung des Projektes VISA - Begrüßung und Einleitung
- 14:00 Uhr Vorstellung des Projektes ESCI - IT-Sicherheit in KRITIS
- 14:45 Uhr Kaffeepause
- 15:00 Uhr Offene Fragerunde zu beiden Projekten
- 16:00 Uhr Abschluss

DECOIT GmbH

Kurze Vorstellung

VISA

Kurzvorstellung der DECOIT GmbH

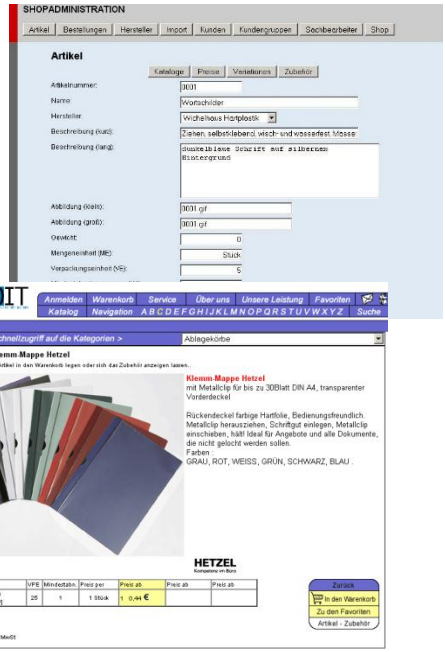
- Gründung am 01.01.2001 als reines Consulting-Unternehmen
- Fokus: Herstellerneutrale, ganzheitliche Beratung
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
- Seit 2002: Systemmanagements, um Herstellerlösungen oder stabile Open-Source-Lösungen anzubieten
- Seit 2002: 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 bzw. Universitäten
- Aktueller Mitarbeiterstand: 15

Dienstleistungen / Portfolio

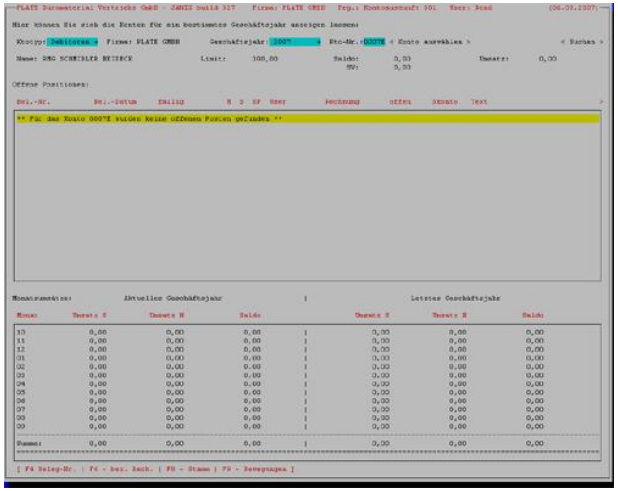
- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** 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

Eigene Produktbeispiele

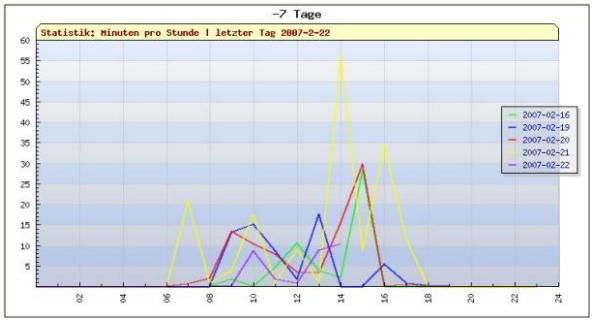
DECO_eShop



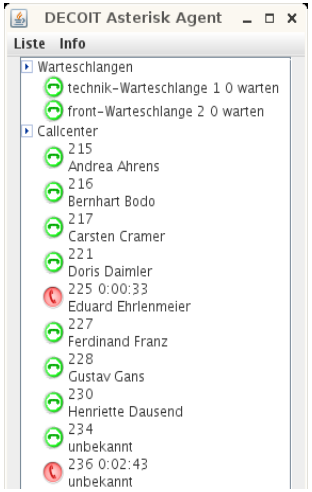
JANIS ERP-Software



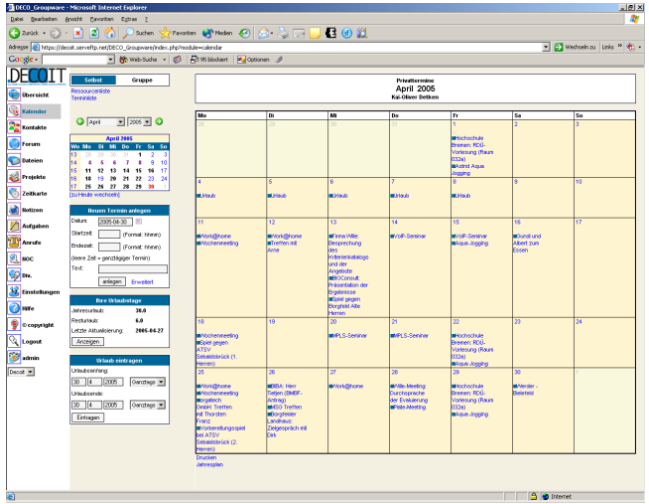
Asterisk Call Detail Records



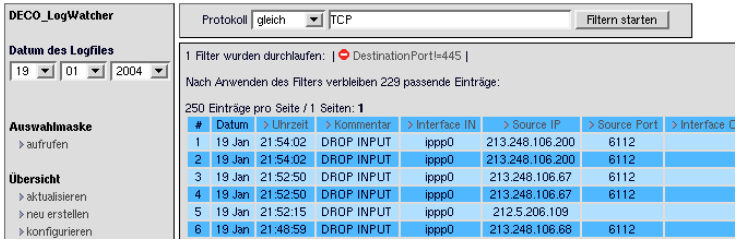
Asterisk Agent Desktop



OSGA - Groupware



DECO_LogWatcher



Forschungsprojekte

Das VISA-Projekt

Eine Einführung

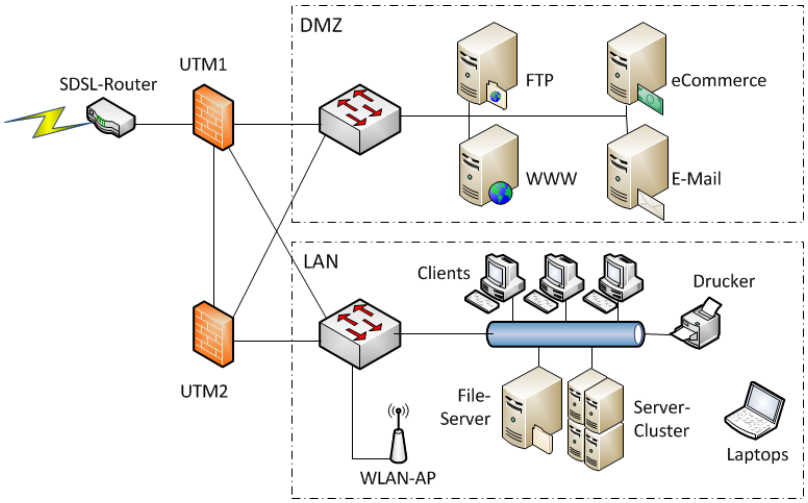
VISA

Projektübersicht

- Das VISA-Projekt startete im August 2011 und wird im Juli 2013 enden
- Es handelt sich um ein BMBF-gefördertes Projekt, mit einem Gesamtvolumen von 1,7 Mio. Euro
- Es sind sechs Partner an dem Projekt beteiligt
  - DECOIT (Konsortialführer) in Bremen
  - Collax GmbH in München
  - Fraunhofer SIT in Darmstadt
  - Hochschule Dortmund in Dortmund
  - IT-Security@Work in Mainz
  - NICTA in Sydney, Australien

Hintergrund des Projektes

- IT-Infrastrukturen sind mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) sehr komplex
- Die Auswirkungen von Änderungen an solchen Infrastrukturen sind oft erst im Echtbetrieb zu erkennen
- Die Integration neuer Sicherheitskomponenten erfordert oft die Integration neuer Hardware und den Umbau der Netztopologie
- Hierbei fehlt oft das entsprechende Wissen in KMUs, so dass Umsetzungen oft ohne eine genaue Kenntnis der Auswirkungen vorgenommen wird



Projektziele (1)

- Vor diesem Hintergrund muss für Klein- und Mittelständische Unternehmen (KMUs) der Umgang mit IT-Infrastrukturen vereinfacht werden
- Dies soll durch den Einsatz von Virtualisierung und Simulation von IT-Infrastrukturen einerseits und durch die Realisierung KMU-gerechter Darstellung und Bedienbarkeit der resultierenden Sicherheitsfunktionalität anderseits erreicht werden
- Es ist daher das Ziel des Projektes VISA, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen insbesondere der Sicherheitskomponenten zu erleichtern und zu unterstützen

Projektziele (2)

- Diese Unterstützung basiert auf zwei Kerntechnologien:
  - Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen
  - Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA)
- Durch das VISA-Rahmenwerk wird der passgenaue und vereinfachte Einsatz von Sicherheitsanwendungen auf Basis von Virtual Security Appliances (VSA) ermöglicht
- Durch die umfassende Emulation der IT-Infrastrukturen können die betriebsrelevanten Parameter und die Integrationspunkte der VSAs bereits in der virtuellen Umgebung identifiziert und der Einsatz erprobt werden

Technische Herausforderungen u. 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

Zwei VSA-Beispiele

VSA-SRC und VSA-MAC

VISA

Technische Herausforderungen u. Ziele

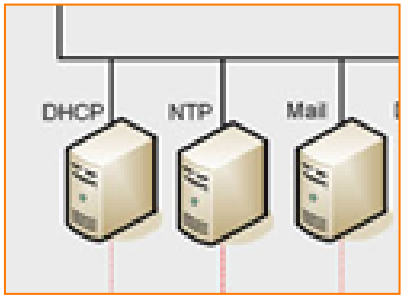
- Definition einer Virtual Machine (VM)
  - Virtueller Computer
  - Ausschließlich in Software umgesetzt
  - Mehrere VMs können auf einem physikalischen Rechner gleichzeitig betrieben werden
- Definition einer Virtual Appliance (VA)
  - Image einer VM
  - Enthält ein installiertes und vorkonfiguriertes Softwaresystem, inkl. Betriebssystem
  - Mehrere VAs können auf einem Server ausgeführt werden
- Definition einer Virtual Security Appliance (VSA)
  - VAs, die vornehmlich der Sicherheit dienen
  - Gleiche IT-Sicherheit wie bei herkömmlichen Lösungen muss gegeben sein
  - Kombination aus diversen VAs

VSA-Bereiche

- **Screened Gateways / Screened Subnets**, die aus kaskadierten Firewall-Strukturen bzw. Kombinationen von Firewalls zusammengesetzt sind (Paketfilter, Proxy, Firewall, Application Level Gateway etc.)
- **Authentisierungsservices**, die i.d.R. aus einem RADIUS-Server oder/und LDAP-Server bzw. Domänen-Controller bestehen
- **PKI-Dienste**, die aus einem CA/RA-Server und optional einem Proxy bestehen

VSA-Eigenschaften

- Was sollten die Komponenten abbilden:
  - Integrierbarkeit
  - Steuerbarkeit
  - Modularität
  - Vergleichbarkeit
- Was sollten die Bereiche abbilden:
  - Konfigurierbarkeit
  - IT-Sicherheit
  - Verfügbarkeit/Migrierbarkeit
  - Autonomie/Adaptationsfähigkeit

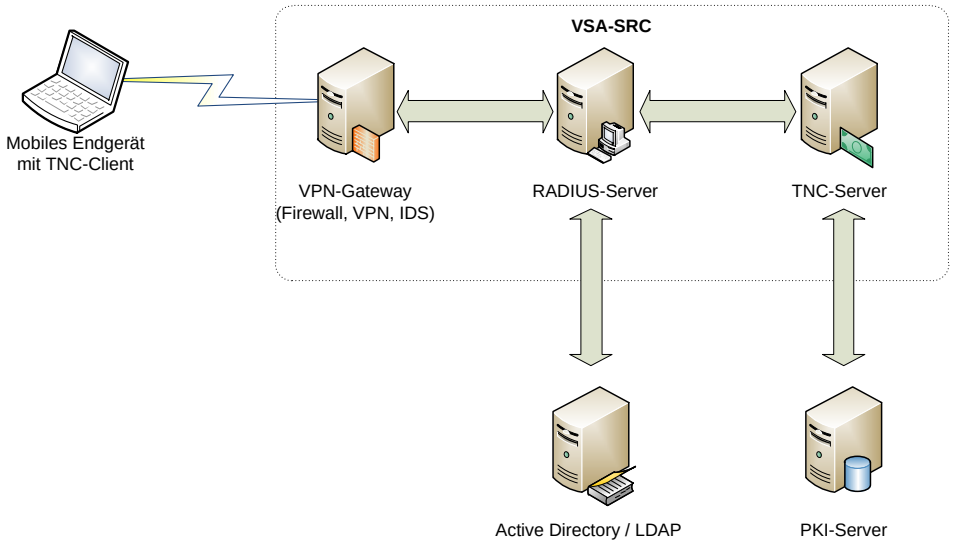


Zwei VSA-Beispiele aus dem Projekt

- **VSA-SRC (VSA Secure Remote Access):** Sicheres Zugriffsszenario von mobilen Endgeräten auf ein Unternehmensnetzwerk.
- **VSA-MAC (VSA Metadata Access Control):** Konsolidierung von Metadaten unterschiedlicher Komponenten zur Erhöhung der Gesamtsicherheit.

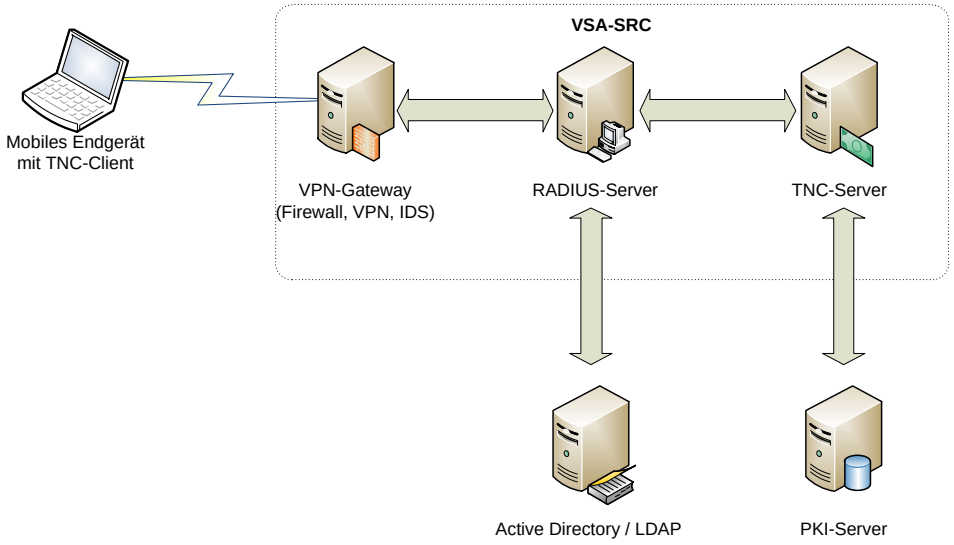
VSA-SRC (1)

- **VPN-Gateway:** Teilnehmer muss sich über einen VPN-Zugang am VPN-Gateway authentifizieren. Damit ist der Login und das Passwort des Teilnehmers zwar abgefragt worden, aber die Hardware kann bereits kompromittiert sein. Daher muss im zweiten Schritt eine Abfrage des TNC-Servers erfolgen.
- **TNC-Server:** Dieser Server nimmt die vom TNC-Client erhaltenen Integritätsmessungen entgegen, die für das mobile Endgerät durchgeführt werden. 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.



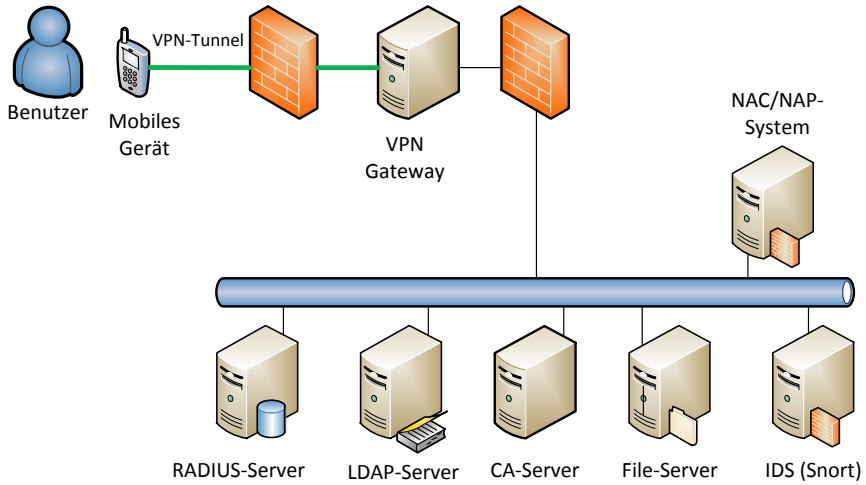
VSA-SRC (2)

- **RADIUS:** Dieser enthält die Einwahlprofile der Teilnehmer, die sich auf das Unternehmensnetz von außen verbinden dürfen. Die Profile enthalten auch die Konfigurationen der jeweiligen Teilnehmer. Eine Synchronisation mit dem internen Verzeichnisdienst wäre sinnvoll.
- **LDAP:** Im Rahmen dieser VSA wird angestrebt, eine Authentifizierung über den Verzeichnisdienst LDAP zu gewährleisten. Dieser bietet eine Unternehmenssicherheit im internen Unternehmensnetz. Außerdem wird angestrebt einen TNC-Server als VA 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. Das VPN-Managementsystem tritt hierbei als Registrierungsstelle (RA) auf. Die VA kann auch erweitert werden, um die Zertifizierung von einer öffentlichen Stelle aus zu übernehmen.



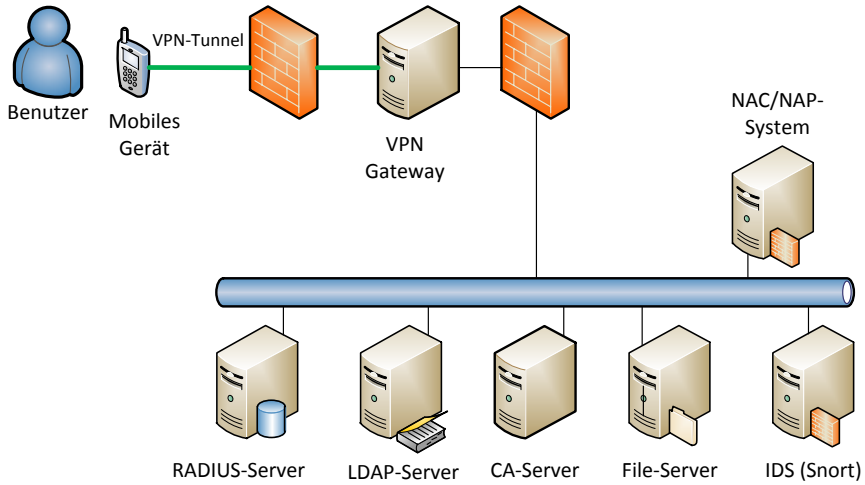
VSA-MAC (1)

- **IF-MAP-Server:** Der 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:** Als Beispiel für den Einsatz des IF-MAP-Protokolls wird eine VA angestrebt, die eine dynamische Konfiguration einer Firewall, basierend auf dem Status des Gesamtnetzes, durchführt. Hierbei werden die Informationen über die Anmeldung eines Gerätes am Netz ausgewertet und in Firewall-Regeln umgesetzt.



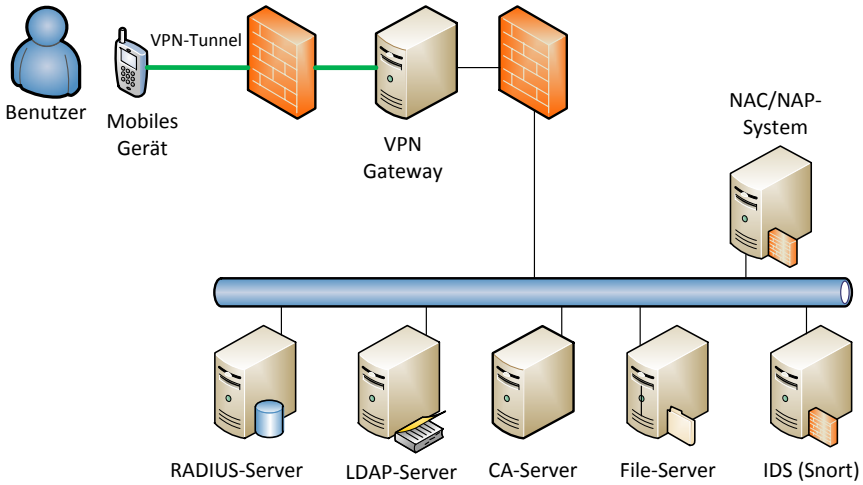
VSA-MAC (2)

- **Android IF-MAP-Client:** Hier soll eine VA 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.
- **Snort IF-MAP-Client:** Der Client beinhaltet die Aufbereitung und Veröffentlichung von Snort-Meldungen. Dies könnte verdächtiger Datenverkehr oder eine Portscan-Erkennung sein. Snort bietet die Möglichkeit Datenverkehr zu analysieren und diesen bei unzulässigen Zugriffen zu unterbinden. Snort ist daher auch als unabhängige VSA zu sehen, die in mehreren Instanzen eingesetzt werden kann.



VSA-MAC (3)

- **RADIUS-IF-MAP-Client:** Dieser Client ermöglicht das Auslesen und Veröffentlichen von RADIUS-Informationen. Auch die Anmeldung und Abmeldung eines Clients werden hier vorgenommen. Sofern eine Authentifizierung gescheitert ist, muss RADIUS diese Information an die Gateway-VA senden. Somit kann die Gateway-VA 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.



VSA-Zusammenfassung

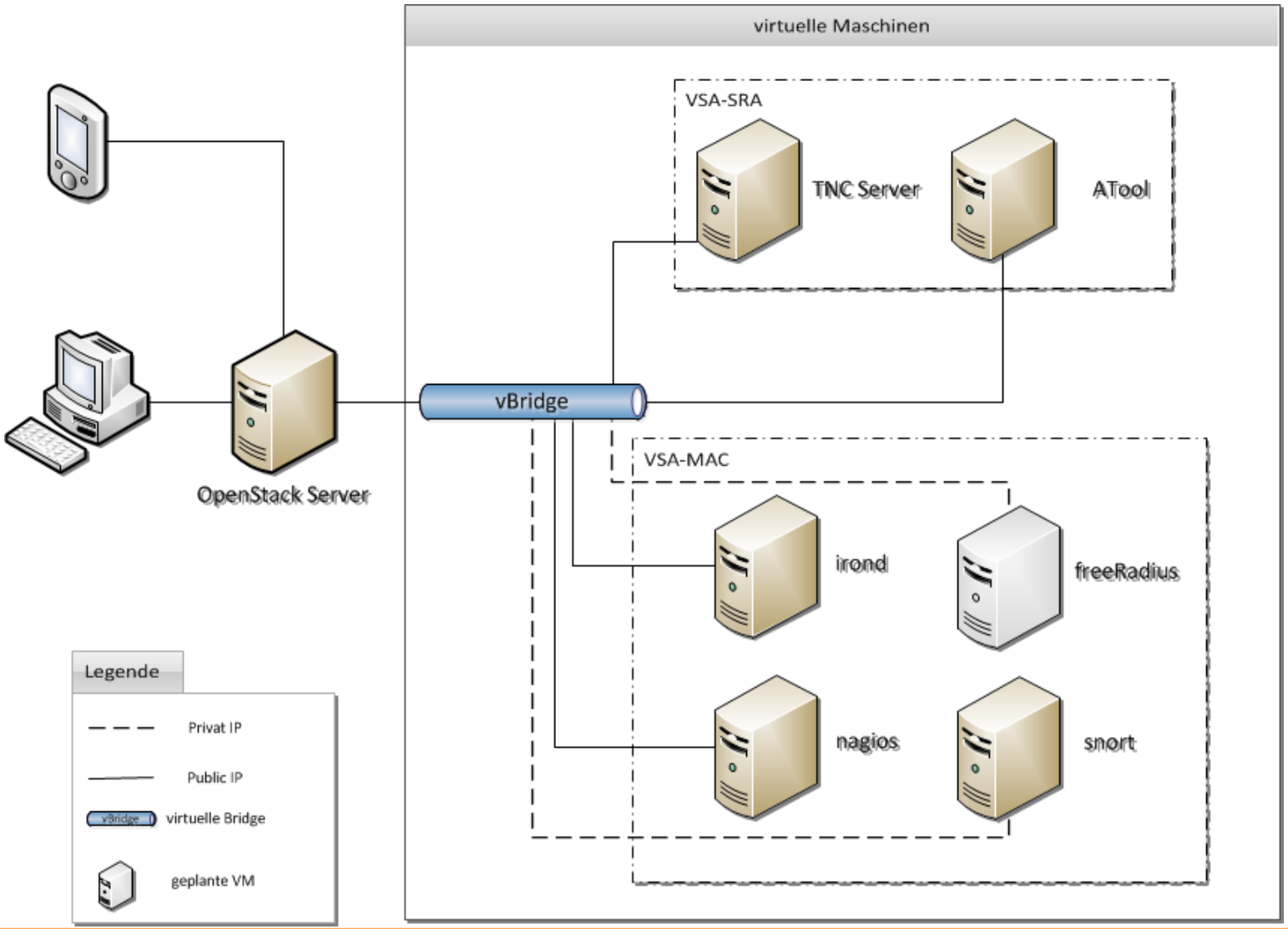
- Beide vorgestellten VSAs sind nun in der Lage eine IT-Infrastruktur für die sichere Einwahl und Nutzung mobiler Endgeräte anzubieten
- Trotz der vielen damit verbundenen Komponenten, lassen sich beide VSAs mit einer entsprechenden Grundfunktionalität installieren, ohne das der Administrator im Einzelnen Bescheid wissen muss, wie ein RADIUS- oder TNC-Server arbeitet
- Dadurch kann die Anbindung mobiler Endgeräte auch in Unternehmensumgebungen erfolgen, in denen der Administrator nicht über entsprechendes Know-how verfügt

VISA-Testbed

bei der DECOIT GmbH

VISA

Aktuelle Testbed-Topologie



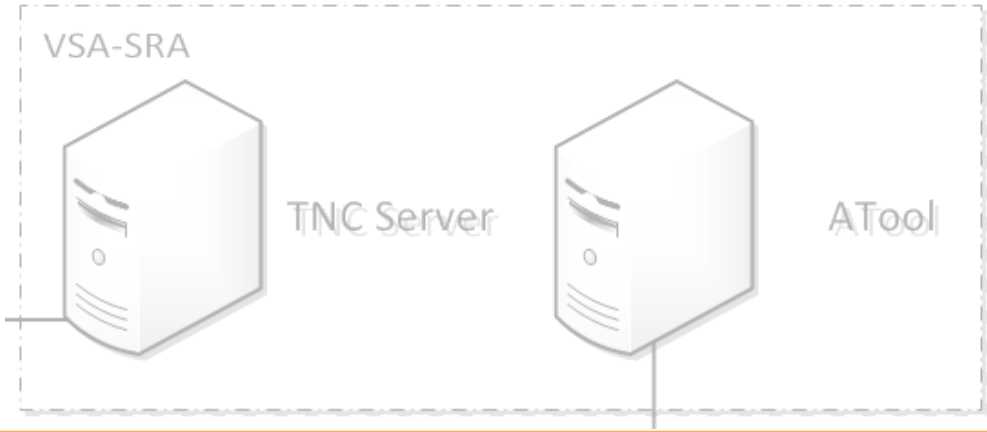
OpenStack-Plattform

- Ohne Quantum
  - Installation auf Ubuntu 12.04
  - Single-Host-Lösung
  - bridge-utils und Nova Network wird für den Netzverkehr der VMs verwendet (kein VLAN-Support)
  - VMs selbst nutzen Ubuntu 11.04
  - VSA-MAC und VSA-SRA sind enthalten
- Mit Quantum
  - Quantum ist ein „Virtual Network Service“, der die Definition von Layer 2 Netzwerkverbindungen zwischen verschiedenen Devices ermöglicht
  - Installation auf Ubuntu 12.04 und Single-Host Lösung
  - Verwendung von Plug-Ins für die Netzwerkverwaltung möglich (Cisco Systems, Linux Bridge, OpenVSwitch etc.)

VSA-SRA (1)

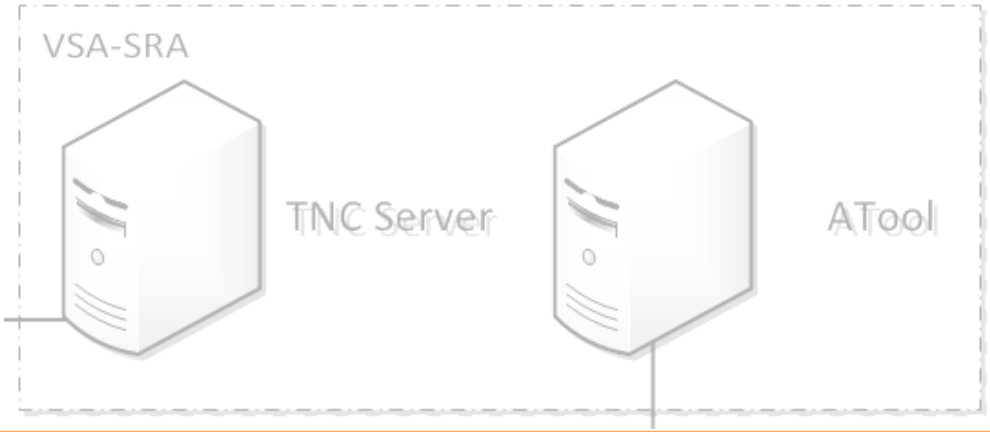
- TNC-Server
  - TNC Server
  - IMV (Integrity Measurement Verifier)
  - CA

  - Dient der sicheren Anbindung eines Smartphone an das Unternehmensnetz



VSA-SRA (2)

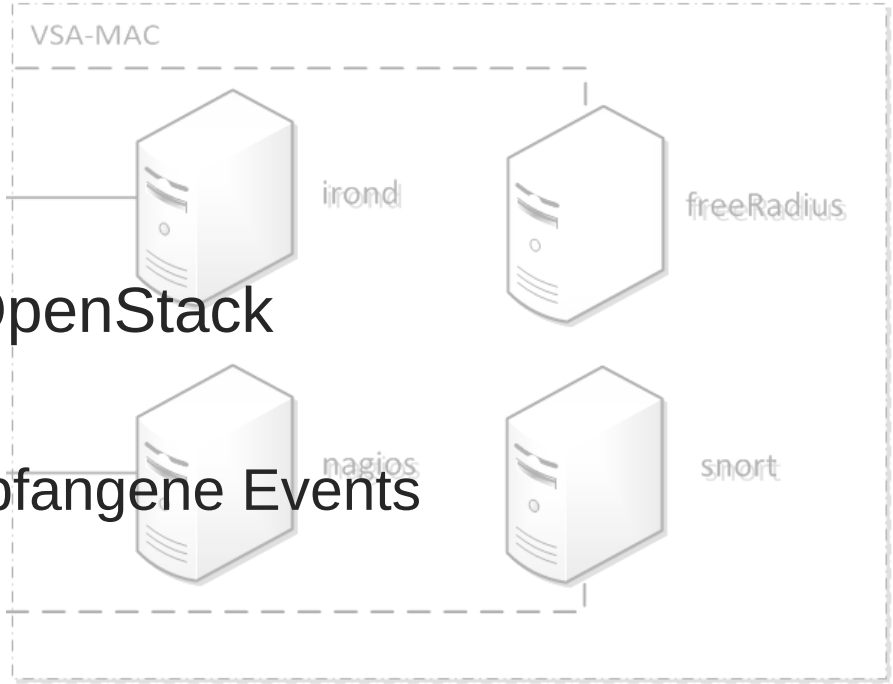
- ATool
  - Webbasiertes Konfigurationstool
  - Speicherung der Konfigurationen in PostgreSQL
  - Überprüft die Syntax der Konfigurationsdateien
  - Erweiterbar für beliebig viele Konfigurationsdateien



VSA-MAC (1)

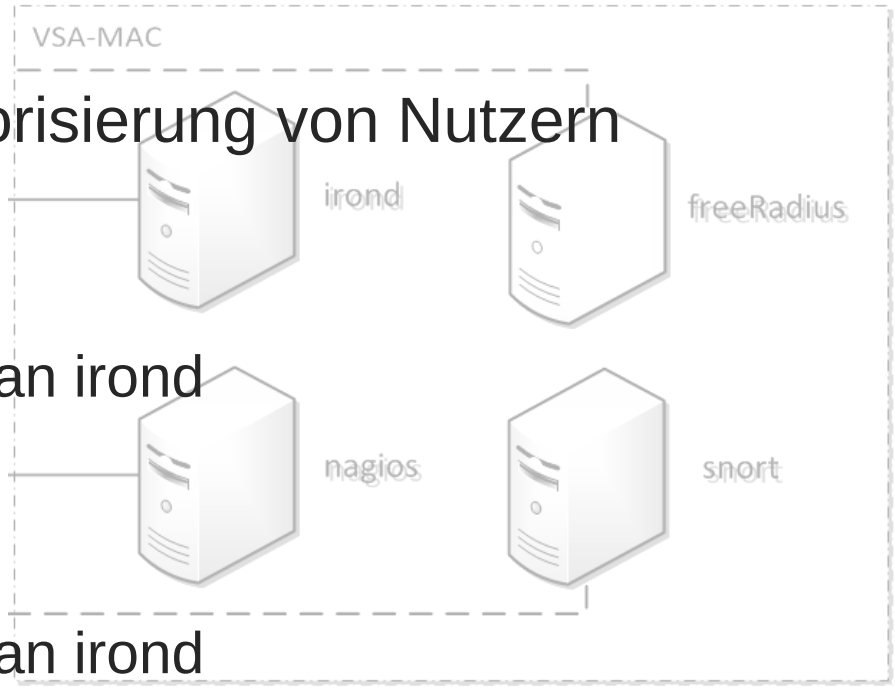
- Irond
  - IF-MAP Server basierend auf JAVA
  - Empfängt / sendet Metadaten
  - Speichert Metadaten in Graphen (irongui)

- Nagios
  - Monitoringsystem
  - Überwacht alle VMs in OpenStack
  - IFMapClient
    - Sendet von Nagios empfangene Events an irond



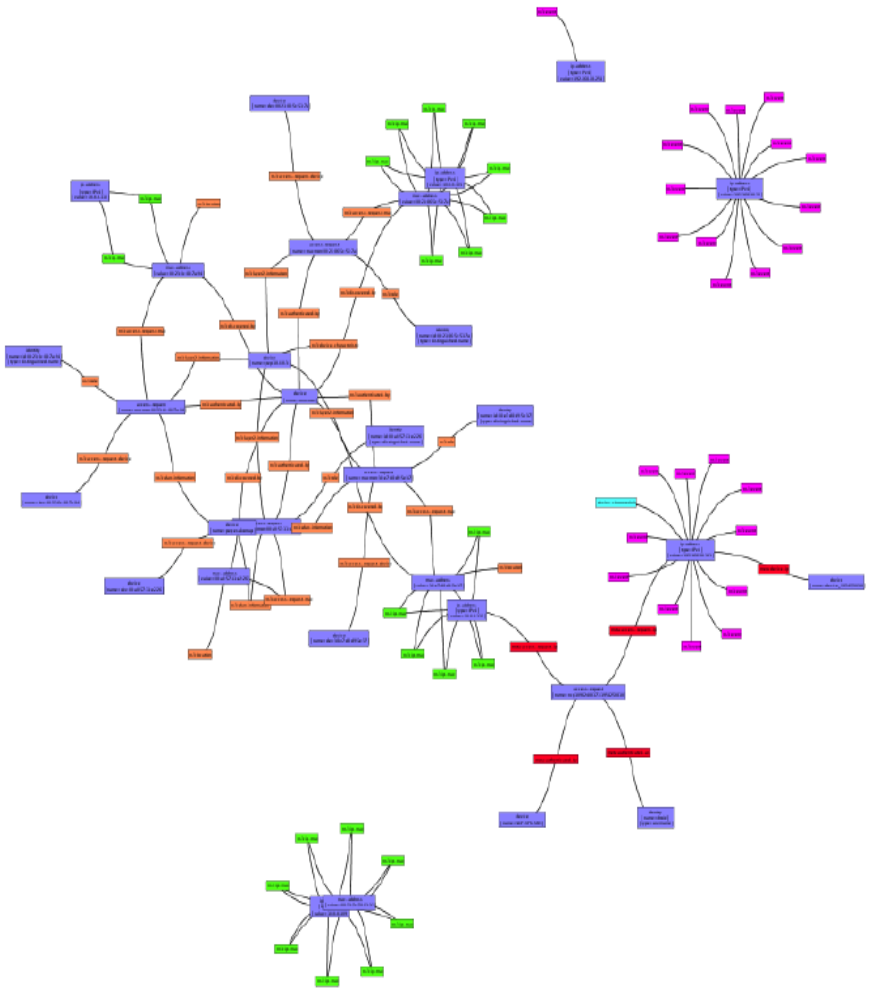
VSA-MAC (2)

- Snort
  - Überwacht Netzverkehr
  - IFMapClient
    - Sendet Vorkommnisse an irond
- FreeRADIUS
  - Authentifikation und Autorisierung von Nutzern und Geräten
  - IFMapClient
    - Sendet Vorkommnisse an irond
- Android
  - IFMapClient
    - Sendet Vorkommnisse an irond



Visualisierung der Netzkommunikation

- Visualisierung von (IF-MAP) Metadatengraphen
  - Anzeige des Metadatengraphen inkl. Zoom-Funktion
  - Einzelne Knoten können ausgewählt werden, um Details über diese anzuzeigen
  - Knoten können per Drag & Drop verschoben werden, Verbindungslinien passen sich automatisch an („Animationsmodus“)
  - Basiert auf Java SE 1.5 und einer Prefuse-Library
  - Apache License 2.0



Zusammenfassung

Status und weitere Arbeiten

VISA

Status

- Testumgebung wurde auf Basis von OpenStack, KVM, libvirt, OpenVSwitch und Quantum aufgebaut
- Zwei VSAs sind in der Testumgebung enthalten, die Forschungsergebnisse aus anderen Projekten weiterführen
- OML-Integration in das Testbed hat in Kooperation mit der NICTA stattgefunden
- Erste Erhebung der virtuellen Testbed-Umgebung hat durch das IO-Tool von Fraunhofer SIT stattgefunden
- Collax hat in seiner VM-Plattform bereits das Managementtool Spotlight entwickelt und integriert

Weitere Arbeiten

- Weitere VSA-Prototypen lauffähig in die Testbed-Umgebung integrieren (FH Dortmund und Collax)
- Zusammenspiel zwischen den verschiedenen VSAs ermöglichen (FHD, Collax, DECOIT)
- Topologie-Editor entwickeln und implementieren (DECOIT)
- OMF/OML-Umgebung integrieren und testen (DECOIT und NICTA)
- Ontologie IO-Tool zur Erhebung und Verbreitung der VSAs erweitern (Fraunhofer SIT)
- IF-MAP in die VSA-SRC integrieren; weitere MAP-Clients entwickeln (DECOIT)
- Compliance-Anforderungen untersuchen und Empfehlungen aussprechen (IT-Security@Work)

Vielen Dank

für Ihre Aufmerksamkeit!

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.