atrete
SOURCING · CONSULTING · ENGINEERING

asut Lunch-Forum

Automatisierung der ICT – nach den Servern die Firewall und das Netzwerk

Anton Klee, CEO & Partner

at rete ag
Eisengasse 16
CH-8008 Zürich

Tel +41 44 266 55 55
Fax +41 44 266 55 88

www.atrete.ch
info@atrete.ch

Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

Wer wir sind

Spezialisiertes ICT Beratungsunternehmen
Eigenständig, unabhängig und neutral
Fokus auf mittlere und grössere Geschäftskunden

- Business Consulting
- Technical Consulting
- Engineering Consulting

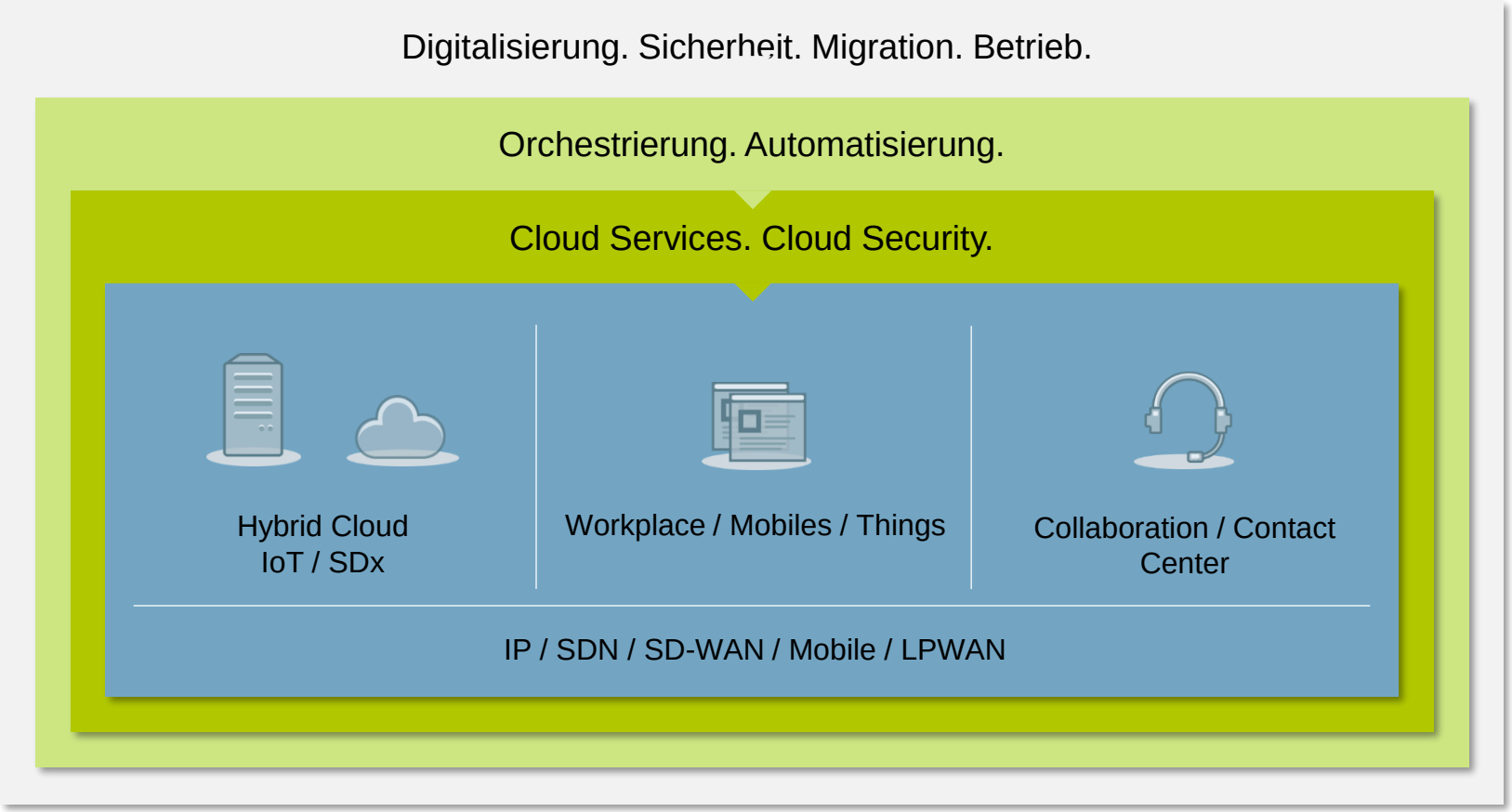
Mitarbeitende	25
Hauptsitz	Zürich, Schweiz
Aktionariat	Partner Modell

1997 — Gegründet im 1997, MBO aus der Electrowatt Engineering AG

1989 — Präsent im Markt seit 1989

atrete
SOURCING · CONSULTING · ENGINEERING

Unser Weg zur Digitalisierung



Was wir tun: ICT Beratung

Strategie	Prozesse	Security Compliance	Sourcing GATT / WTO	Engineering
Planung	Design	Analyse	Anforderungen und RFP	Technische Konzepte
Implementation	Implementation	Architektur	Vertrag	Implementierungs-anleitungen
Review	Review	Implementation	Verhandlung	
	Optimierung	Audit	Transition	

Projektleitung (PRINCE2 zertifiziert)

Personalverleih / Interim Management

Unsere Kunden

Finanz, Versicherung

- AKB
- Credit Suisse
- Helsana
- LGT Group
- Privatbank
- Swiss Life
- Swiss Re
- Visana
- ZKB

Pharma, Chemie

- Geistlich
- Givaudan
- Roche
- Takeda
- Novartis

Öffentlicher Sektor

- Kanton Aargau
- Kanton Luzern
- Kanton Zürich
- Schweizerische Bundesverwaltung
- SRG SSR
- Stadt Zürich OIZ
- Stadt Kloten
- Switch
- ZID Basel Stadt

Transport

- SBB
- Flughafen Zürich AG

Logistik

- Schweizerische Post
- Swissport

Gesundheit

- Medbase

Industrie, Retail

- Forbo
- OC Oerlikon
- Mettler-Toledo
- Migros
- SFS
- Sika
- Sulzer
- Victorinox

Provider, Energie

- Abraxas
- BKW
- ewz
- ewb
- IWB
- Groupe e
- Sunrise
- Swisscom
- Swissgrid

Bildung

- ETH Zurich
- Universität Basel
- Universität Zürich
- FHNW

Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

Automatisierung – oder «ICT industrialized»
Schnittstelle zwischen ICT Angebot und Leistungserbringung

Kunden – Orientierung

ICT-Angebot:

Applikationen
- Biz-Apps
- ERP
- Office Apps..

Plattformen
- Mainframe
- Server-Plattformen
- Middleware

Workplace
- Desktop I, II
- Mobile I, II

Communication
- Fix-Voice
- Mobile-Voice
- Mobile Data/Voice
- Connectivity I,II

'Industrielle' Fertigung:

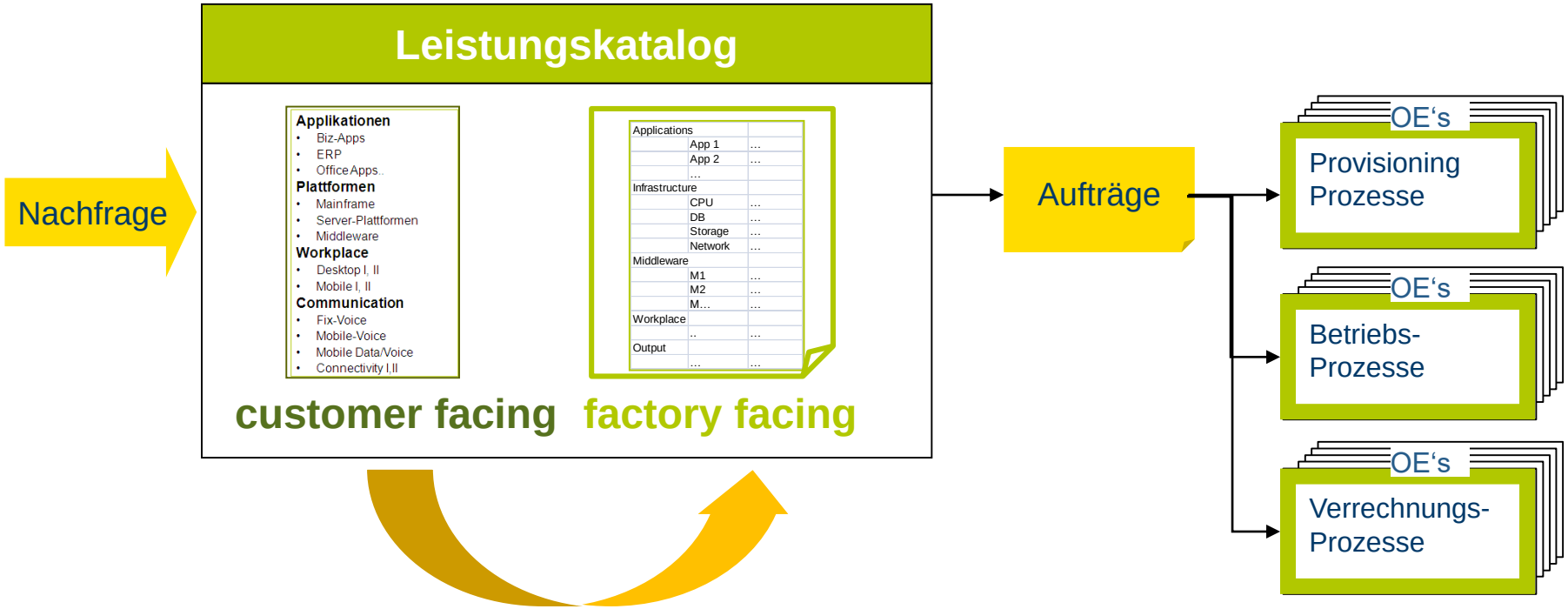
Standards für:

→ Provisioning / Changes

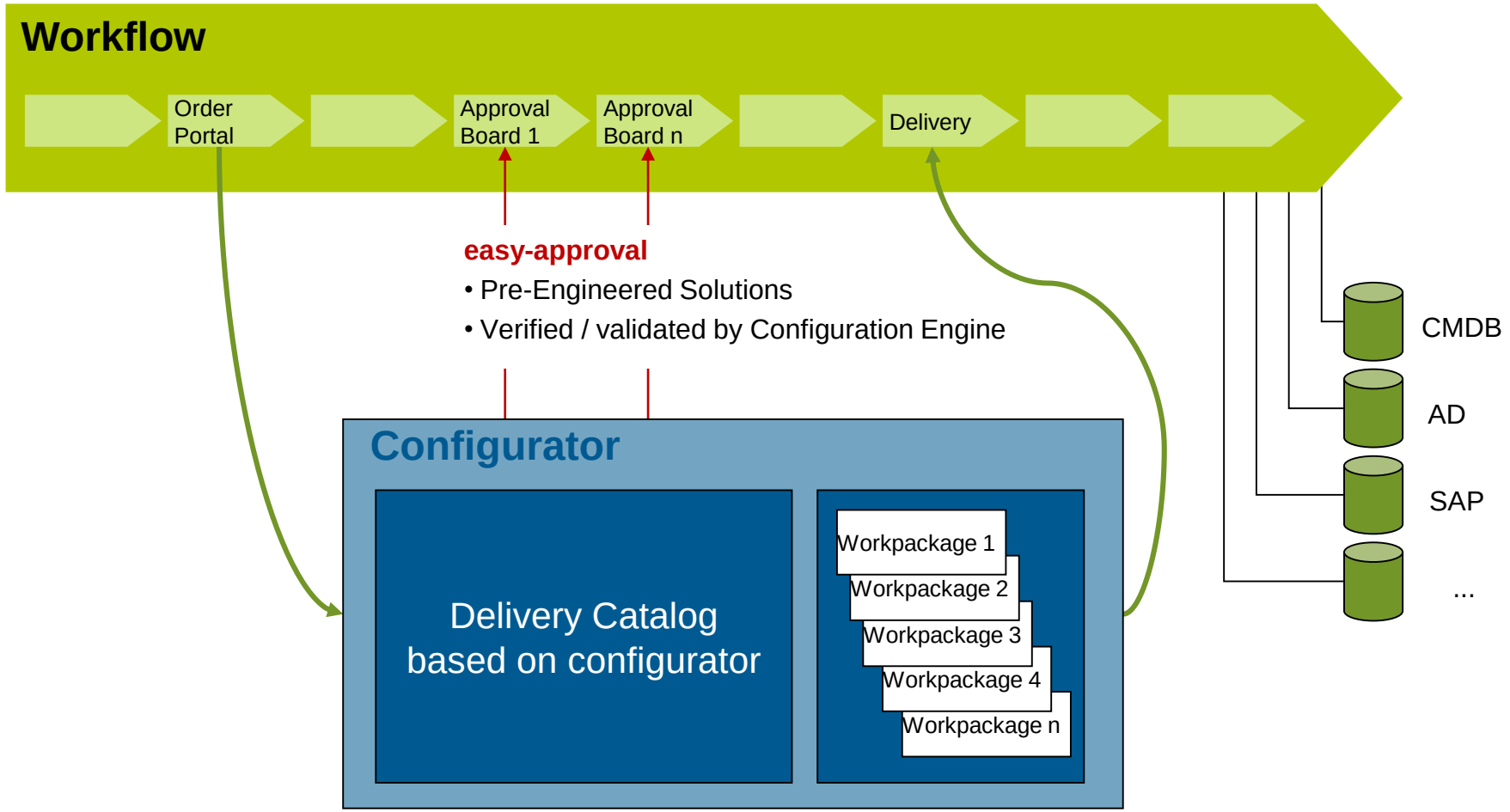
→ Betrieb

→ Verrechnung

Unterscheidung von ‘Customer-’ versus ‘Factory’-facing



Erste Ansätze von Automatisierung durch Prozess-Integration



Hürden auf dem Weg zur Automatisierung
… und deren disruptive Auflösung

Hürden:

- Organisationen / Zuständigkeiten / R&R
- Plattform-Vielfalt: HW und SW…
- Unterschiedlichste Konfig-Tools…

Disruption:

- Die Virtualisierung – weg von physischen Instanzen!
- Software Defined *anything*
- Cloud Anbieter für Compute/Storage Leistungen treten auf

Virtualisierung im Server-Umfeld

Abstraktion

Abstraktion der Server Hardware gegenüber dem Betriebssystem

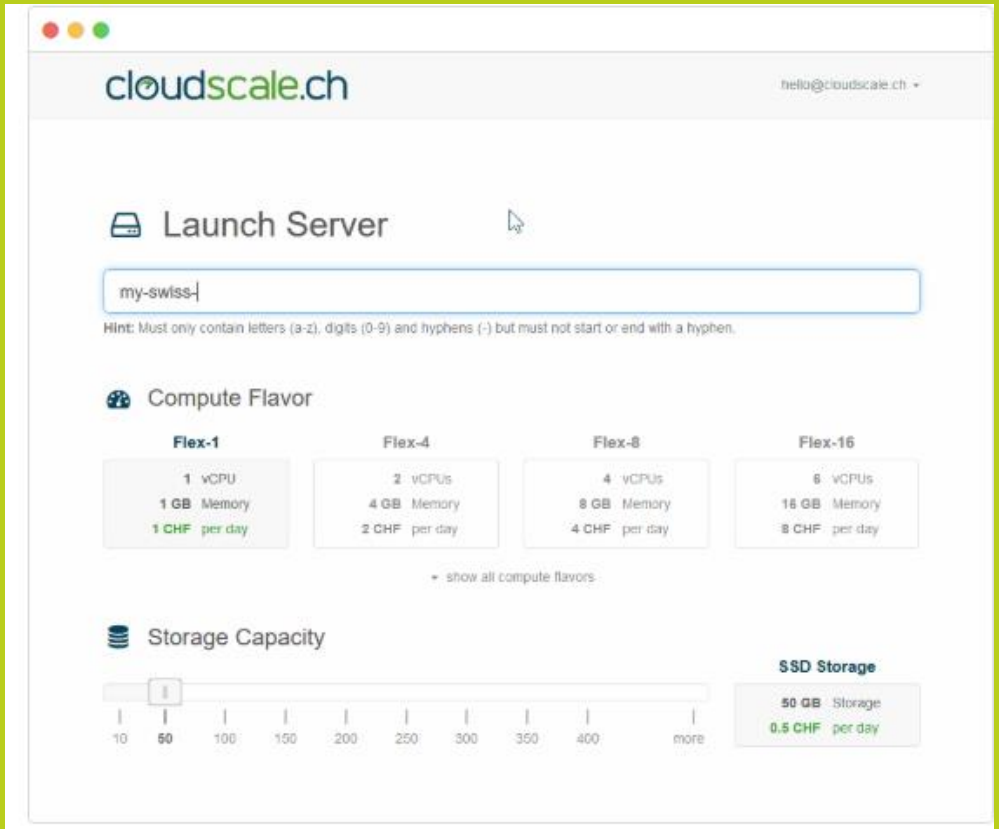
- Unabhängigkeit von der Hardware
  - Standardisierte Schnittstelle gegenüber OS
  - Pooling von Server Ressourcen auf standardisierten Hardware Plattformen
- Portierbarkeit von OS-Instanzen
  - als File
  - on the fly (vMotion, Live Migration, …)

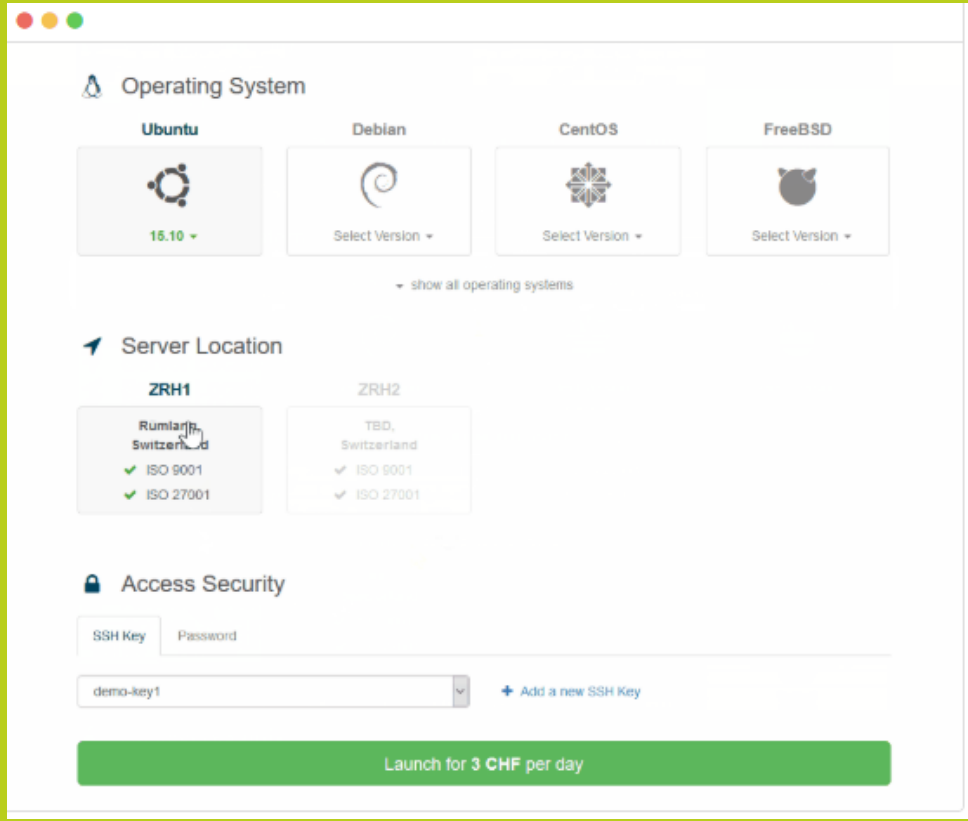
Orchestrierung

Zentrale Orchestrierung der Ressourcen

- zentrales Management
- übersichtliche Administration vieler Server
- wenige Clicks für Server Instanzierung
- Skalierung der Ressourcen im Betrieb

Und die realen Umsetzungen … Server Bestellung on-the-fly





Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

Wie sieht’s denn beim Netzwerk aus?

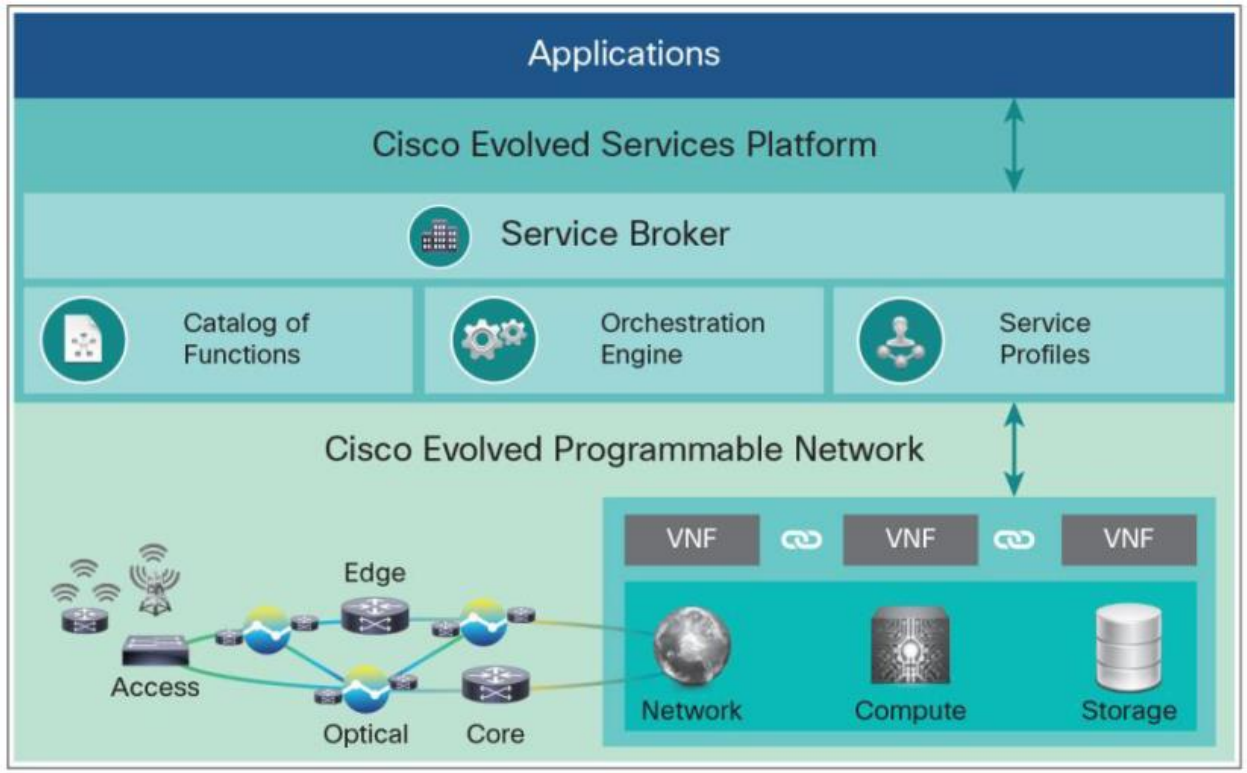
Lassen sich auch Netzwerke / -komponenten virtualisieren?

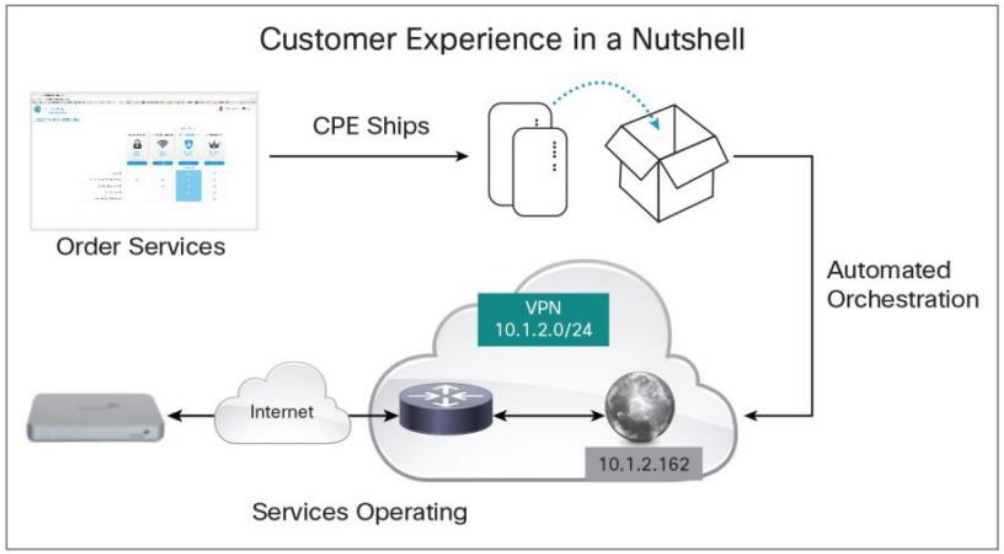
Aussage aus dem Jahre 2015

«The network is constraining the full realization of the power of the virtualization»

Mike Marcellin, Senior VP, Strategy and Marketing, Plattform System Division, Juniper Networks

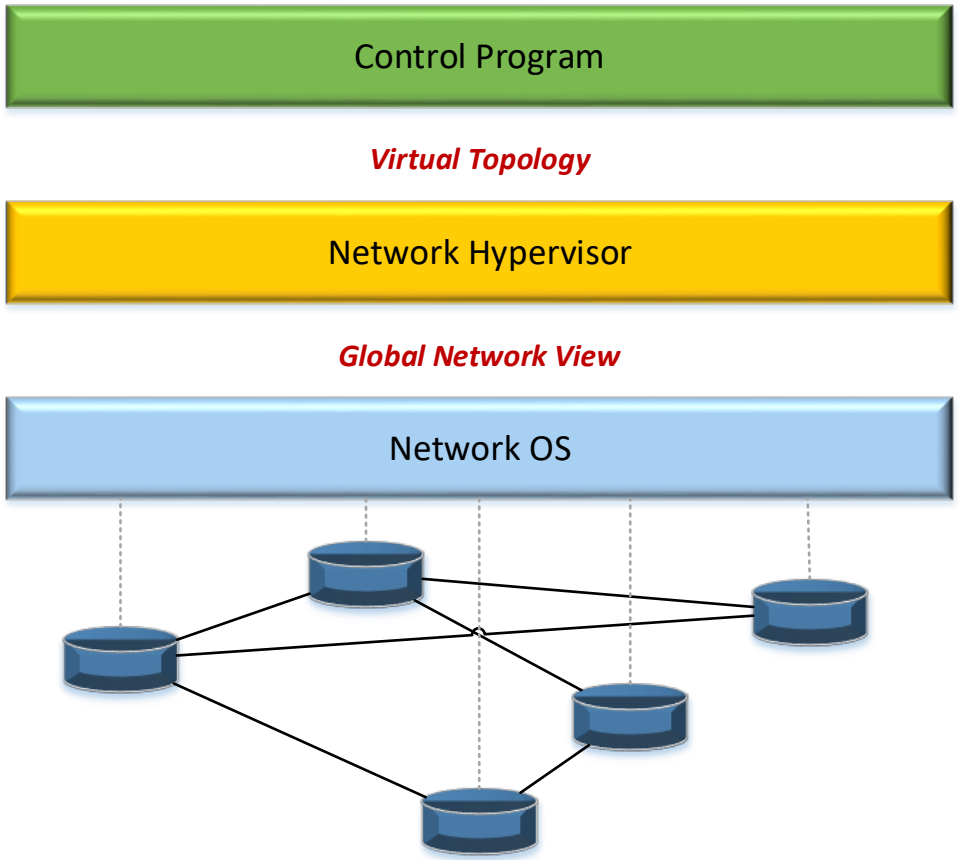
Damaliger Ausblick des Branchenleaders (2015)



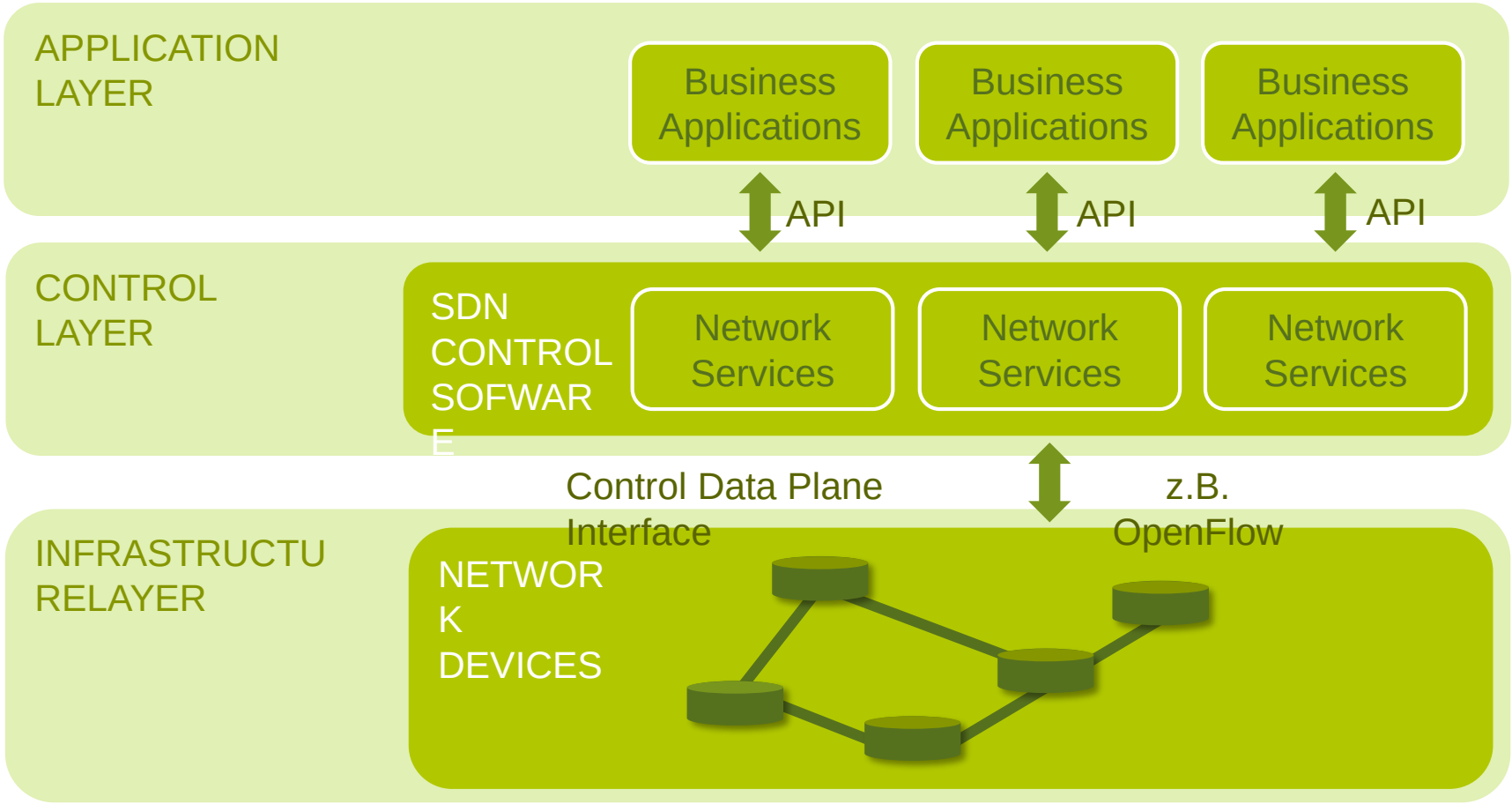


Software Defined Networking

SDN Virtualisierungsmodell

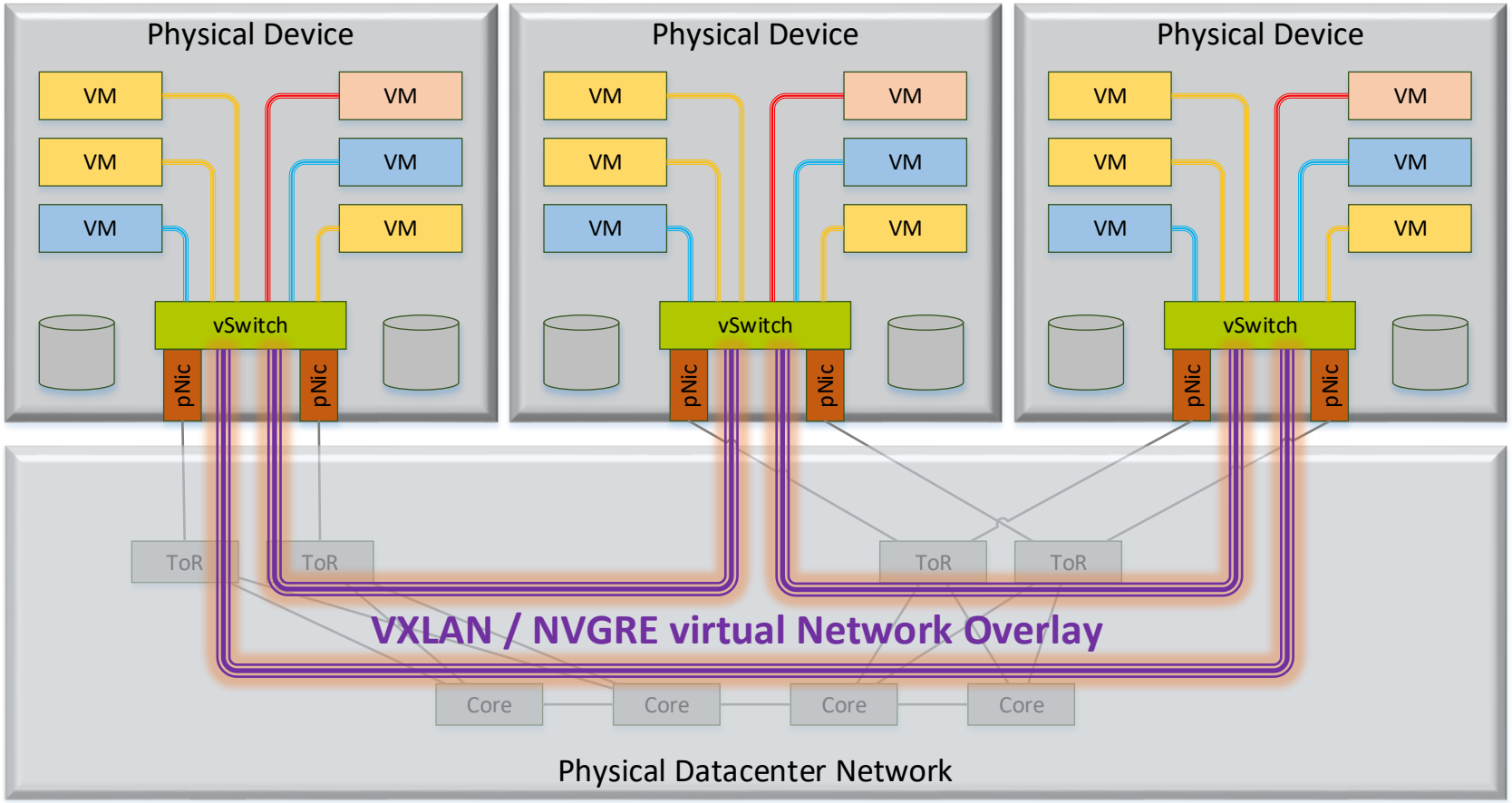


SDN Architektur



Software Defined Networking

Network Overlay



Charakteristik der SDN-Architektur gemäss Open Network Foundation

- **Agil**
- **Zentral gesteuert**
- **Programm gesteuert –**

  „SDN ermöglicht dem Netzwerk-Manager eine schnelle und einfache Verwaltung von Netzwerk-Ressourcen (configure, manage, secure, optimize) mittels dynamischen und automatisierten Programmen.

  Diese können einfach selbst entwickelt werden, da sie nicht von proprietärer Software abhängig sind.“

Die SDN Welt – und deren Begrifflichkeiten…

Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

Automatisierung – was?

Provisionierung

Automatisierung als Teil von Provisionierung

- Public Cloud (AWS, Azure, …)
- Private Cloud
- DC vs. Access/Sites
  - Zonen, FW, Load-Balancing/Proxy
  - SDA (Software Defined Access)

Operations

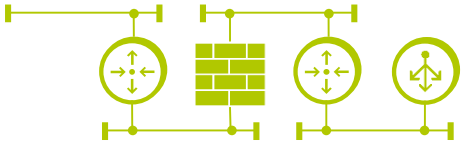
Automatisierung als Teil von Operation
(real time)

- SD-WAN
- Traffic Engineering

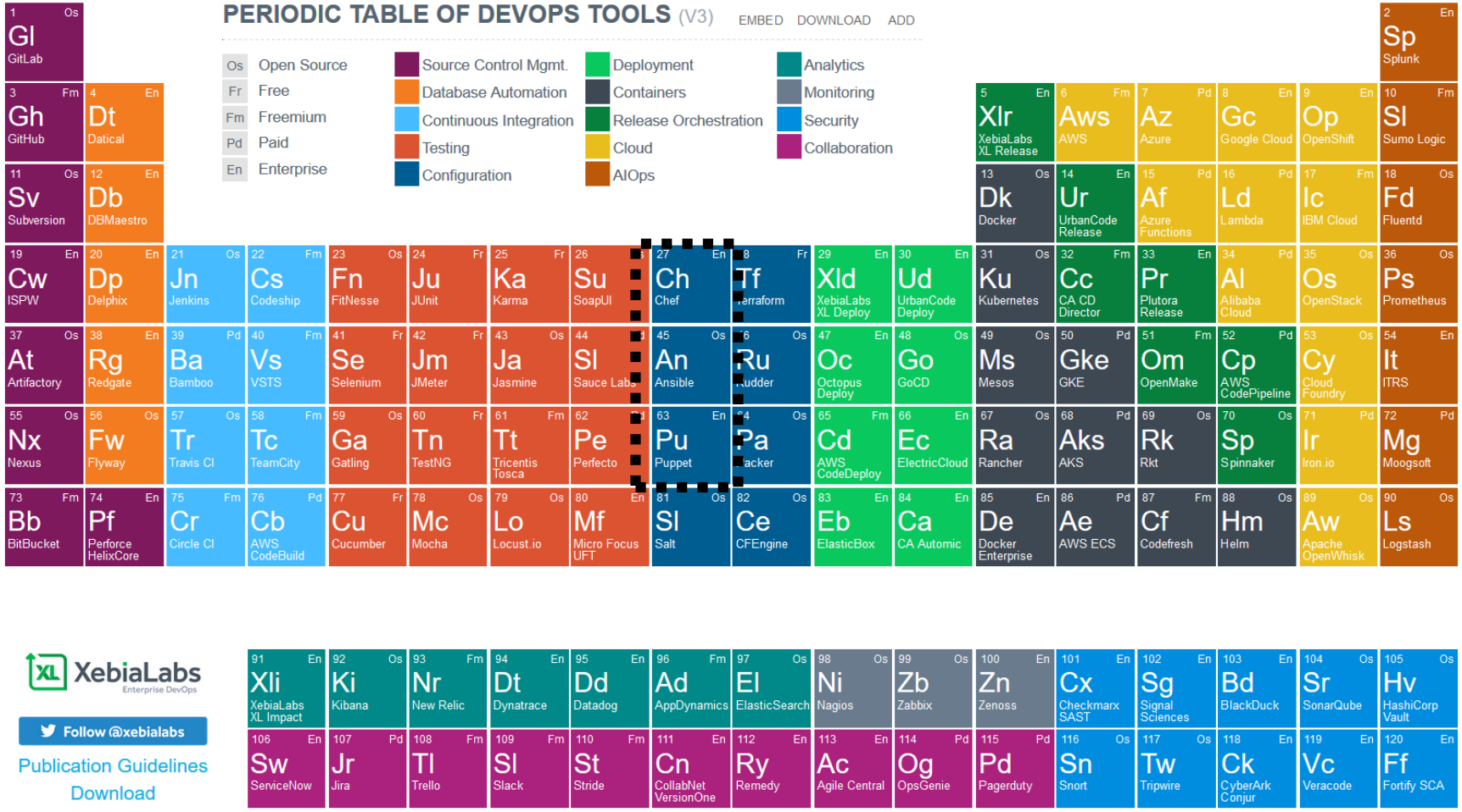
Konfiguration

Automation von immer wiederkehrenden Konfigurationen/Services

Automatisierung nach Infrastruktur-Komponenten – Stand heute

Paas & SaaS		Bereitstellung von SW-Komponenten und Einstellungen für unterschiedliche Systeme für den Setup einer ganzen Applikation • **zur Zeit eher selten**
Compute & Storage		Bereitstellung kompletter Compute-Systeme (virtuell und physisch) mit unterliegenden Speicher und OS-Komponenten • **Häufig: automatisierte Bereitstellung von VMs basierend auf vordefinierten OS-Builds**
Firewall & ProxyRules		Workflow-basierter Prozess für Bewilligung UND Deployment von FW Rule Change Requests • **Automatisierung noch nicht häufig gesehen**
Network		Bereitstellung von Netzwerkressourcen. Moderne Infrastrukturen bieten API (SD…) • **(noch) nicht häufig genutzt** • **heutige "Automatisierung" basiert meist auf einzelnen Skripts, Serienbriefen und Excels**

Periodensystem von DevOps Tools



https://xebialabs.com/periodic-table-of-devops-tools/

Konfigurationsmanagement und Automation Frameworks/Libraries

Puppet

- One of the oldest solutions in the market
- Ruby
- Manifests
- **Agent-based**

«Auf dem Server läuft ein zentraler Puppet-Daemon (*puppetmaster*), der die Konfigurationen der Rechner vorhält und auf Anfrage via REST-API austeilt. »

Chef

- Ruby
- Recipes (Cookbooks)
- **Agent-based**

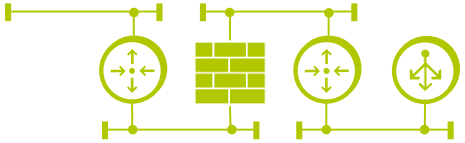
«Chef is used to streamline the task of configuring and maintaining a company's servers, and can integrate with cloud-based platforms such as Internap, Amazon EC2, Google Cloud Platform… »

Ansible

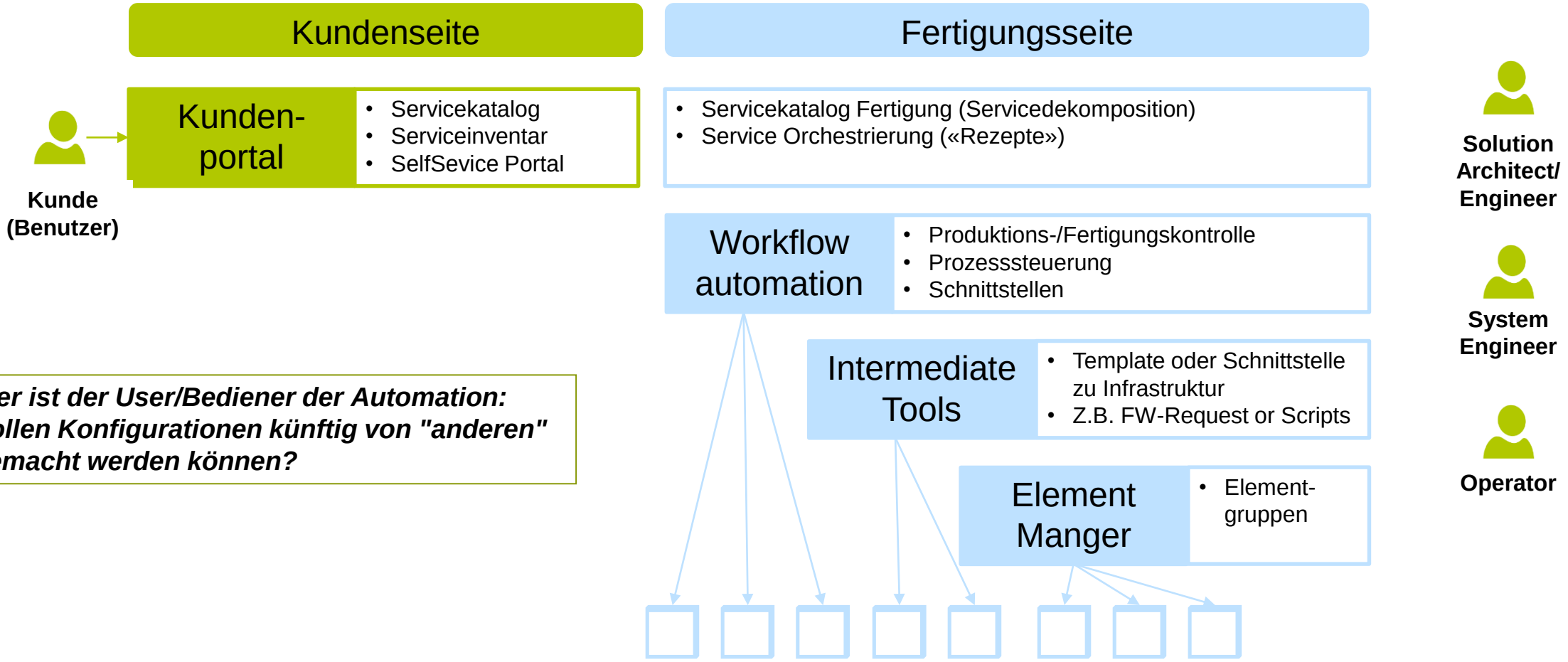
- Not only a Configuration Management System
- Python
- Playbooks
- **Agent-less**

«Ansible ist ein Open-Source Automatisierungs-Werkzeug zur Orchestrierung und allgemeinen Konfiguration und Administration von Computern. Es kombiniert Softwareverteilung, Ad-hoc-Kommando-Ausführung und Konfigurationsmanagement»

Automation auf verschiedenen Ebenen – unterstützende Tools

Paas & SaaS		• AWS, Azure, OpenStack • *IBM Cloud Orchestration / BPM* • *Cisco Cloud Orchestrator / UCS Director*
Compute & Storage		• vRealize • *Ansible, Chef, Puppet*
Firewall & ProxyRules		• Tufin • *Algosec* • *Skybox*
Datacenter Network		• Ansible, Python • IBM Netcool Configuration Manager • Solarwinds network configuration Manager • NetMRI, Cisco Prime • ACI, NSX
Access Network		• SDA, SD-WAN (Vendor specific solutions) • Ansible, Python • NSO

Architektur der Automatisierung



Wer ist der User/Bediener der Automation: Sollen Konfigurationen künftig von "anderen" gemacht werden können?

Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

BEISPIEL AUTOMATISIERUNG

Vollständig automatisierte Provisionierung von virtuellen Netzwerkressourcen im Datacenter

Automatisierungsumgebung

Netzwerk

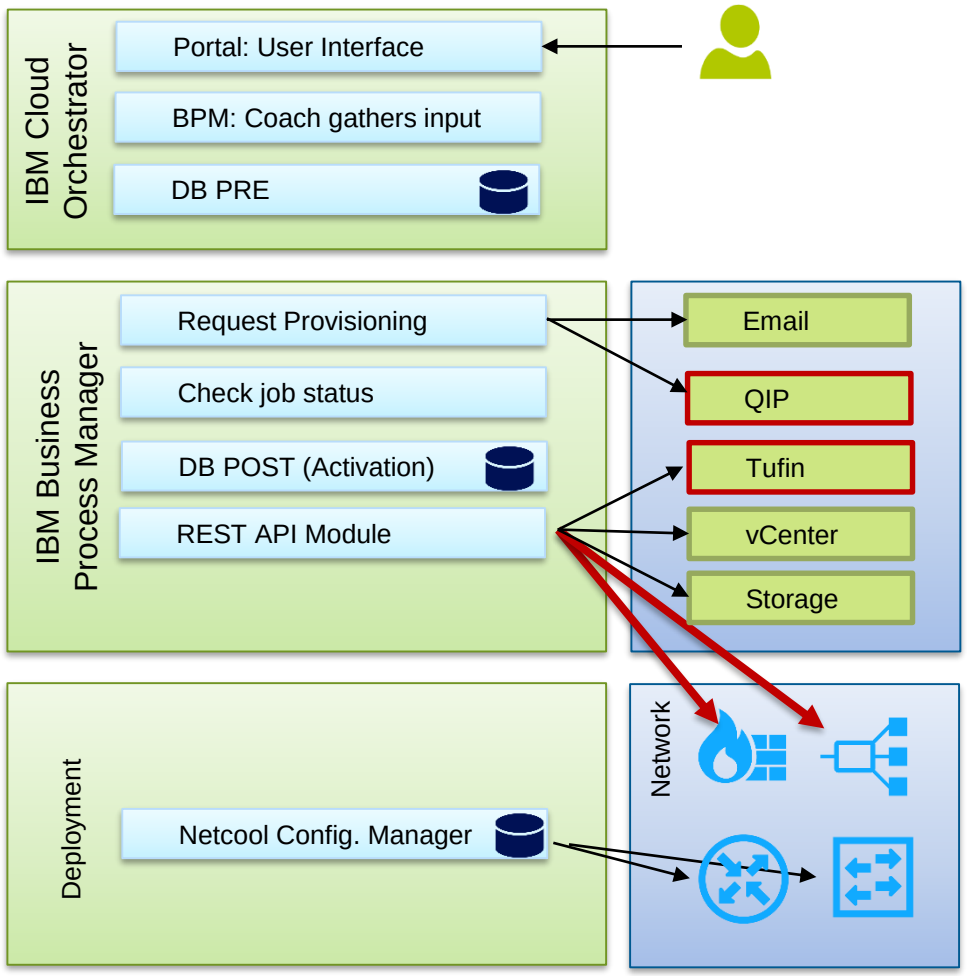
- MPLS-/VLAN-basierte Netzwerkarchitektur
- Automatisierte/virtualisierte Netzkomponenten (vNF): Switch, Router, Firewall, Loadbalancer
- Standardisierte/modularisierte Servicekomponenten werden vom Solution Engineer zu End-to-End Netzwerkservices verbunden

Ziel der Orchestrierung/Automatisierung

- Automatisierter Roll-out von definierten Connectivity Services
- Realtime Dokumentation der konfigurierten Services
- Durchsetzung von standardisierten Konfigurationen
- Umsetzung virtualisierter Servicearchitektur und -design, welche nur mit Einsatz von Automatisierung zuverlässig betrieben werden können

Beispiel eines User Interfaces

Applikations-Komponenten



ICO: GUI, Benutzerportal und Self-Service Offers (Servicekatalog und Servicemodule)

BPM: Businesslogik und Schnittstelle zur Fertigung

NCM: Roll-out Netzwerkkonfiguration (klassische Netzwerkkomponenten)

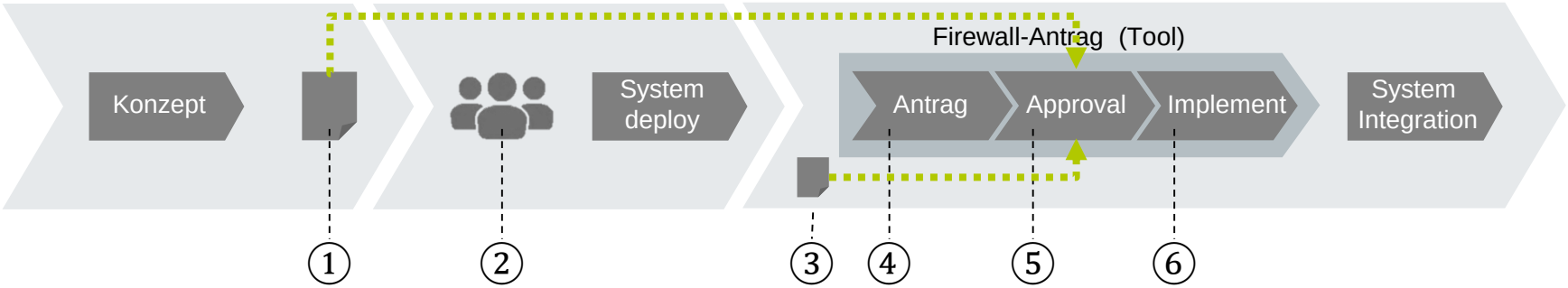
Projekt Herausforderungen

- Software Engineering trifft auf System Engineering
- Spezifikation / gemeinsames Verständnis
- Schnittstellen und Abhängigkeiten
- Agile Software Development, regelt Priorität nur bedingt das Lieferdatum
- Ad hoc Changes

Agenda

1. atrete
2. «ICT industrialized»: Die frühen Stadien
3. SDN everywhere
4. Automatisierung generell
5. Netzwerk
6. Firewall-Rules Antragsprozess
7. Unsere Empfehlungen zur Automatisierung

Firewall-Antragsprozess

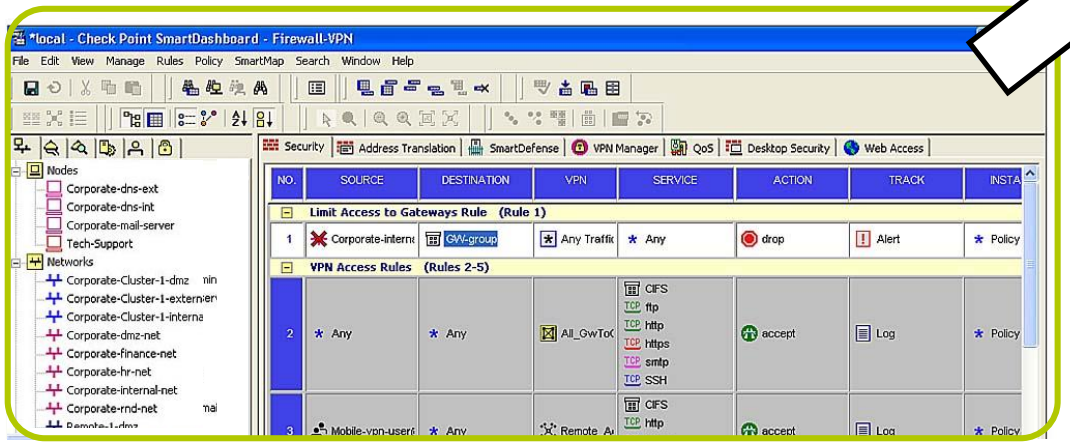


ID	Beschreibung
①	Festlegung der Platzierung durch eine Design/Architekturstelle zu prüfen und freizugeben. Resultate dieser Prüfung sind im Antragstool anzuhängen, als Grundlage für die Beurteilung eines Antrags.
②	Bereitstellung Ressourcen gemäss Platzierung: Zuordnung von IP-Adresse und Systemnamen. Neue Systeme müssen in den korrekten Netzwerkzonen bereitgestellt werden.
③	Zusätzliche Bewilligungsgrundlagen im Antragstool bereitstellen (Bsp. Kundenvereinbarungen, Ausnahmegenehmigungen, etc)
④	Einreichen Firewall-Antrag: Ein konkreter Antrag für Firewallregeln kann erst eingereicht werden, wenn die Namen und IP-Adressen der Systeme bekannt sind.
⑤	Beurteilung Firewall-Antrag: technische Plausiblität und Sicherheitsrisiko jeder einzelnen Verbindung anhand einer konfigurierbaren Risikomatrix. Flexibler Workflow leitet Antrag zur passenden Bewilligungsinstanz weiter. Antragstool zeigt «kritische» Verbindungen auf, Beurteilung und Bewilligung basieren jedoch auf vorhandenen Grundlagen (siehe ① und ③) und erfolgen typischerweise manuell.
⑥	Freischalten der Verbindungen in der Firewall: Bewilligte Anträge werden in der Infrastruktur implementiert (manuell / automatisch). Der Antragsteller wird bei jeder Statusänderung informiert (Bsp. „Antrag implementiert“).

Von der «Firewall-Regel» hin zur «Verbindung»

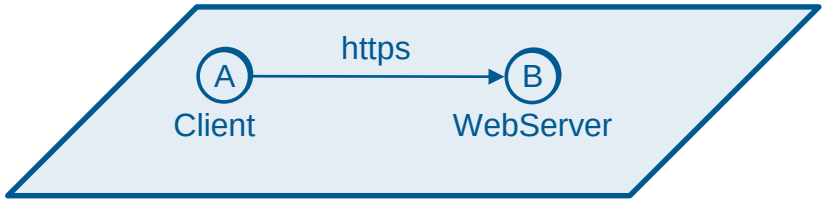
Neuer Ansatz: benötigte Verbindungen zwischen Endpunkten bestellen
→ **Verbindungs-orientiert**

Quelle: Tufin Orchestration Suite



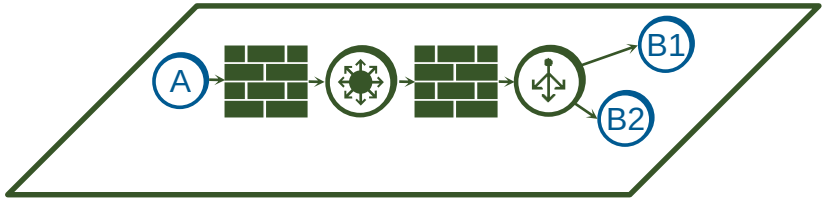
Was wir heute typischerweise tun:
einzelne Regeln auf spezifischen Firewalls erstellen → **Enforcement Point orientiert**

Trennung von Verbindungs- und Enforcement Ebene



Verbindungs-Ebene

Logische, applikationsorientierte Verbindungen



Abbilden auf Topologie-Map

Feststellen, welche Komponenten im Routingpfad involviert sind

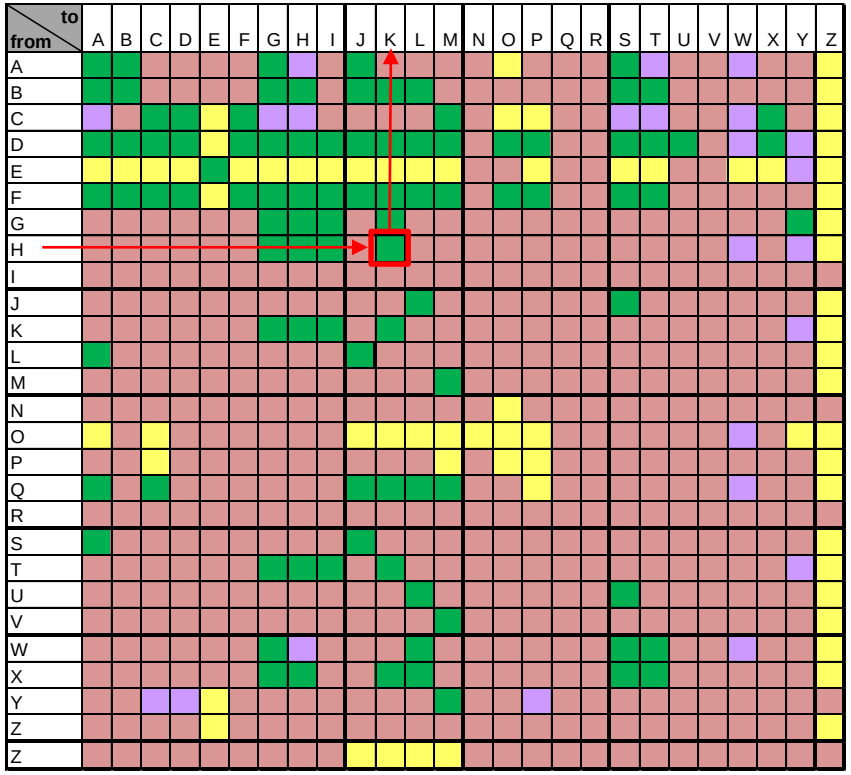
✓ Schon freigeschaltet ⊗ blockiert

Enforcement-Ebene

Analyse und Verwaltung der technischen Policies der Enforcement Points (Produkte)

→ Unabhängigkeit der technischen Umsetzung von der logischen Verbindung

Compliance Prüfung anhand einer Policy/RiskMap



Beispiel von Zone H nach K: «low Risk»-Verbindung und daraus folgend z.Bsp. «auto approval» (keine manuelle Bewilligung notwendig)

- Risikobewertung jeder Verbindung am Zonenübergang.
- Festlegung der Zonen im Antragstool notwendig (IP-Bereiche).

- Flexibler Risiko- und Workflowprozess, gesteuert durch (u.a.):
  - Verwendete Services
  - Spezifische Source / Destination
  - Anzahl IP's beantragt
  - Firewalls im Pfad
  - Bearbeiter
  - …

low risk
high risk
medium
suspected

atrete
SOURCING · CONSULTING · ENGINEERING

Tipps für erfolgreiche Automatisierung

- Bedürfnisse müssen bekannt sein
- Prozesse müssen bekannt sein
- Bereitschaft für Veränderung
- Offen für neue Lösungen

Ausblick für weitere Einblicke – zB SDN Konferenz

SDN NFV WORLD CONGRESS 2018

The World's meeting place for Network Transformation
NFV+SDN & Automation for 5G, Transport & Cloud

8-12 October 2018 | World Forum, The Hague, Netherlands

SDN NFV WORLD CONGRESS | ACCELERATING INNOVATION FOR NETWORKS

1. **Technology** – Cloud-Native NFV, Hybrid, Interop, SDN, White box, Security
2. **Automation** – AI, Zero Touch, Orchestration, Programmable Cloud, OSS/BSS, API
3. **Business** – 5G, Services Transformation, SD-WAN, Application use-cases

Dedicated Forums are organised at this year's Congress, in order to bring focus to key developmental topics, to form a unique meeting point for these communities, and to support collaboration to advance the work: