Bundesrepublik Deutschland
Finanzagentur GmbH

Beyond Technology: Die Rolle von Prozessen und Management bei der Firewall-Integration

Alexander Vogt, Finanzagentur, IT-Sicherheitsbeauftragter
Daniel Rehnitz, Finanzagentur, Gruppenleiter Netzwerk
Tim Klotzback, Controlware, Technical Consultant

17.09.2025, Congress Park Hanau

1 Der große Traum

2 Die Bedarfsplanung

3 Die Realisierungsplanung

4 Die Umsetzung

Der große Traum

- Wir wollen sicher sein
- Wir wollen uns kontinuierlich verbessern
- Wir wollen moderne Technik betreiben
- Wir sind state of the art

Das böse Erwachen

- Wir brauchen mehr Personal
- Wir brauchen mehr Budget
- Wir brauchen mehr Zeit
- Wir brauchen einen Plan

1 Der große Traum

2 Die Bedarfsplanung

3 Die Realisierungsplanung

4 Die Umsetzung

Bedarfsplanung

Wie wollen wir segmentieren?

Was ist in den nächsten Jahren realistisch realisierbar?

Wollen wir auf einen Schlag ein segmentiertes Netz?

Was macht technisch überhaupt Sinn?

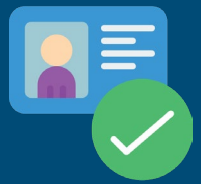
Wie wollen wir segmentieren?

Zonenbasiert

Gerätebasiert

Anwendungsbasiert

Identitätsbasiert



Bedarfsplanung

Wie wollen wir segmentieren?

Was ist in den nächsten Jahren realistisch realisierbar?

Wollen wir auf einen Schlag ein segmentiertes Netz?

Was macht technisch überhaupt Sinn?

Was macht technisch überhaupt Sinn?

- **Unternehmensgröße**
- **Ausgangslage**
- **Compliance**
- **Weiteres…**

Bedarfsplanung

Unternehmensgröße

Small Business

Medium Business

Enterprise

Ausgangslage

OT/ICS

Network Design

Status

Compliance

- NIS 2
- DORA

Weiteres...

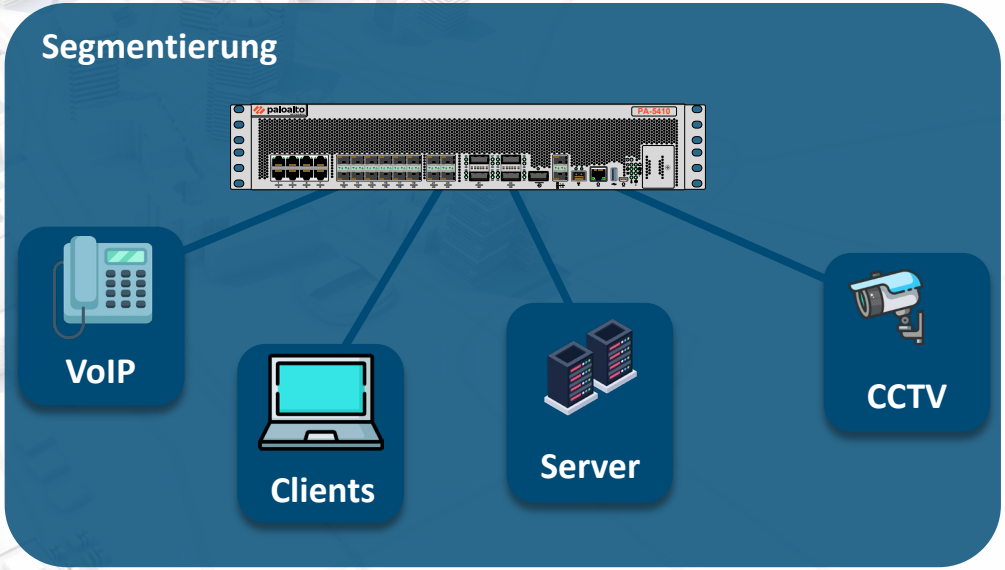
Budget

DDoS/Downtimes

Personal

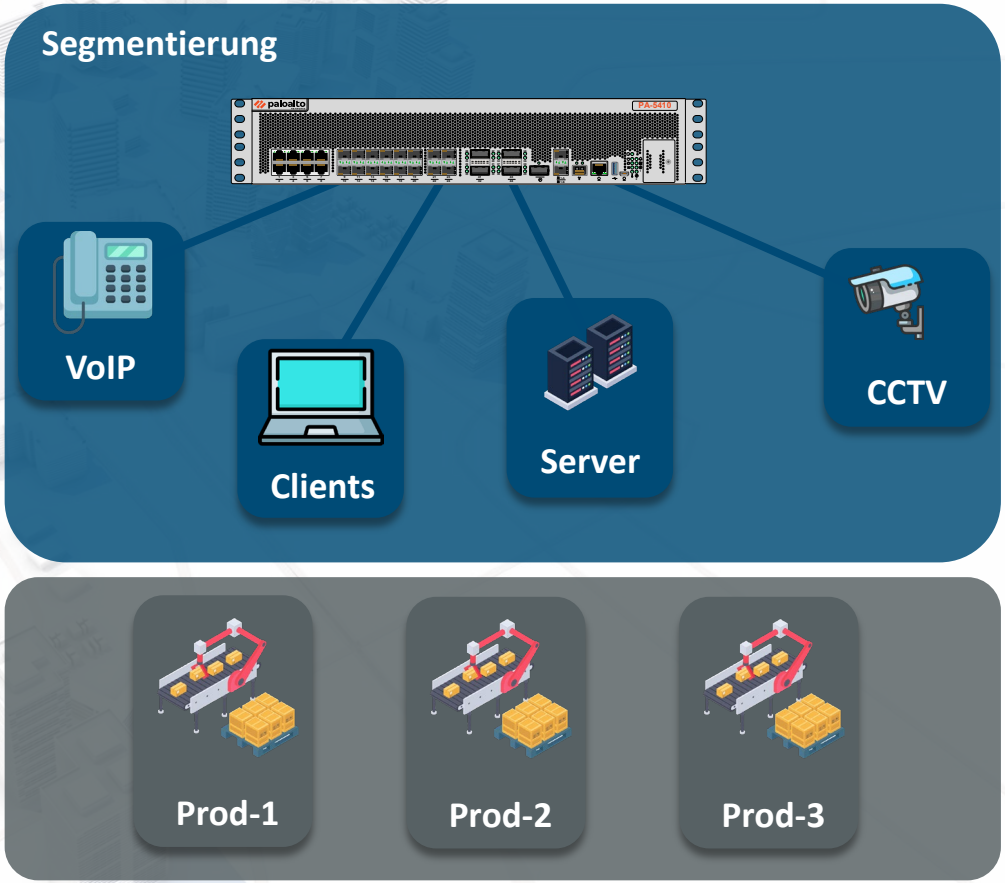
Bedarfsplanung

- Ein Beispielaufbau mit Perimeter und Segmentierung…
- Was mache ich mit meiner Produktion?



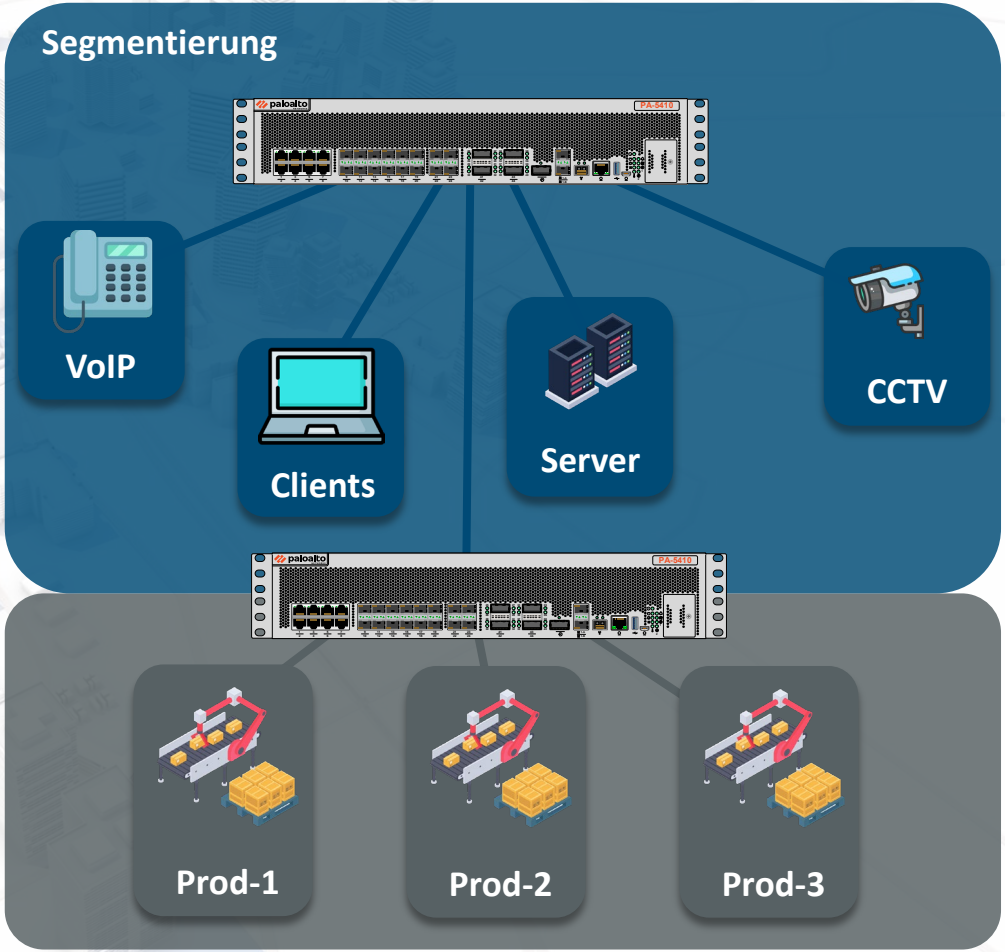
Bedarfsplanung

- Ein Beispielaufbau mit Perimeter und Segmentierung…
- Was mache ich mit meiner Produktion?



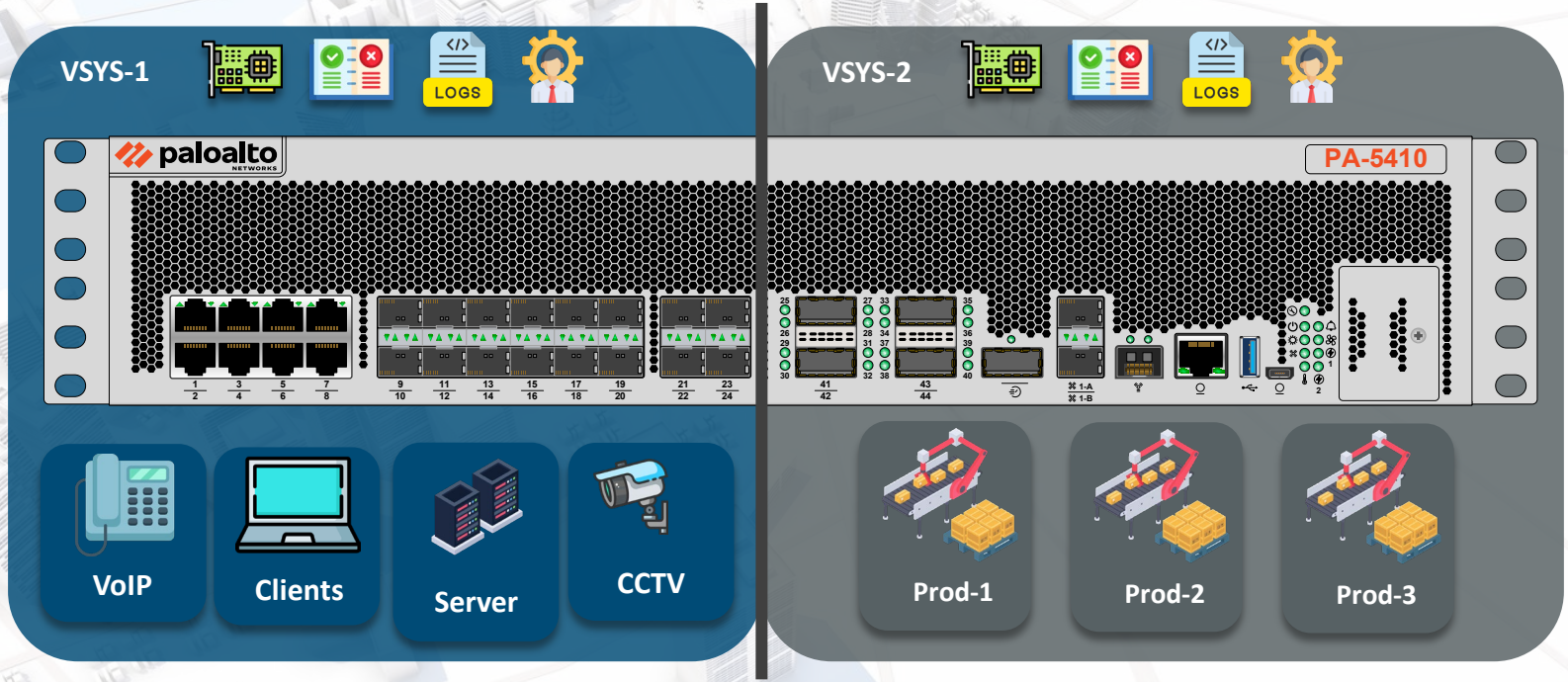
Bedarfsplanung

- Eine neue Firewall…
- **Geht das auch anders?**



PAN-OS | Virtual Systems

- Eine Trennung der physischen Firewall in virtuelle Instanzen



Was macht technisch überhaupt Sinn?

- **Unternehmensgröße**
- **Ausgangslage**
- **Compliance**
- **Weiteres…**

Bedarfsplanung

Wie wollen wir segmentieren?

Was ist in den nächsten Jahren realistisch realisierbar?

Wollen wir auf einen Schlag ein segmentiertes Netz?

Was macht technisch überhaupt Sinn?

Was ist in den nächsten Jahren realistisch realisierbar?

Infrastruktur?

ToDo´s?

Team?

Bedarfsplanung

Wie wollen wir segmentieren?

Was ist in den nächsten Jahren realistisch realisierbar?

Wollen wir auf einen Schlag ein segmentiertes Netz?

Was macht technisch überhaupt Sinn?

Wie
segr

Wollen wir auf einen Schlag ein segmentiertes Netz?

VS

.

ächsten
tisch
ar?

chnisch
Sinn?

Bedarfsplanung

Wo

segm tz?

Was ist in den nächsten Jahren realistisch realisierbar?

Was macht technisch überhaupt Sinn?

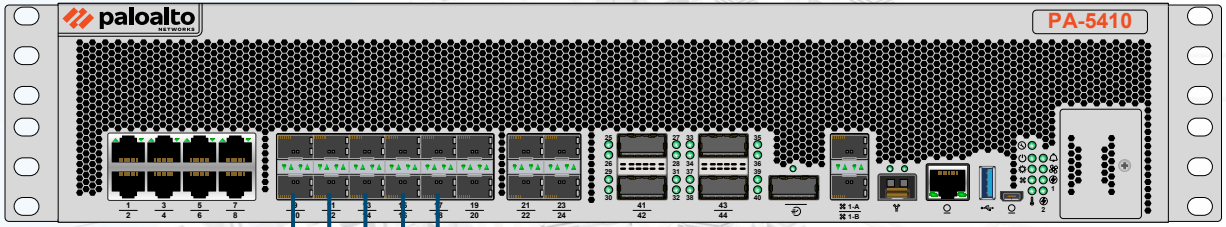
1 Der große Traum

2 Die Bedarfsplanung

3 Die Realisierungsplanung

4 Die Umsetzung

Realisierungsplanung



Netzdesgin

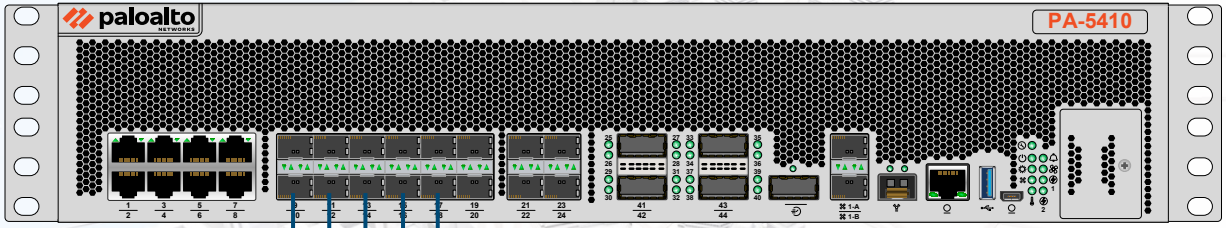
Segmente

IP-Konzept

Prozesse

Werbung

Realisierungsplanung



Netzdesgin

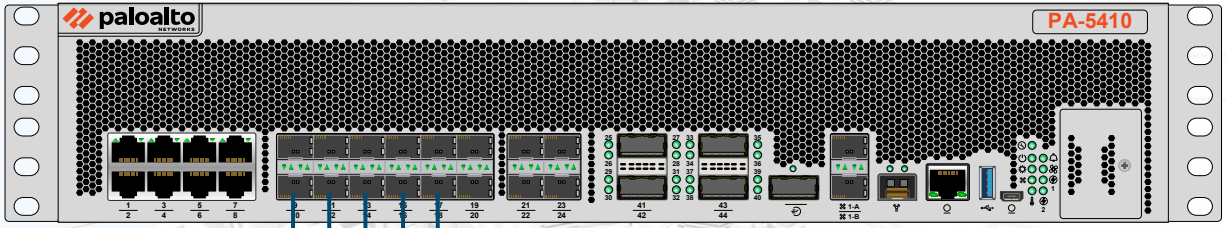
- Performanceplanung
- Integrationsplanung
- Portplanung
- Leitungsplanung

Prozesse

IP-Konzept

Werbung

Realisierungsplanung



Segmente

- Segmentierungskonzept
- Segmentierungsregeln
- Segment-Eigner
- Umsetzungsplan

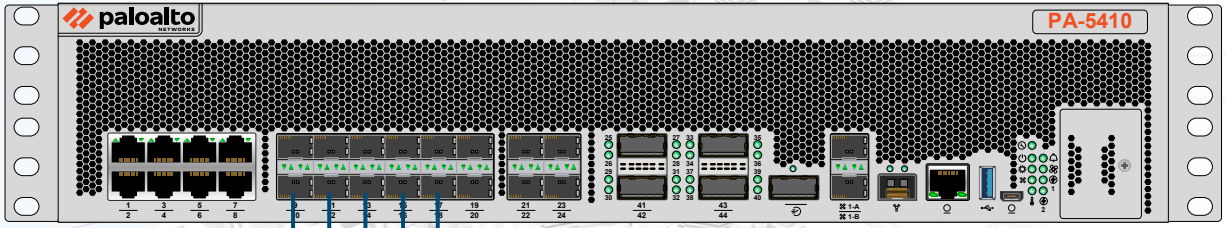
Ne

IP-Konzept

Prozesse

Werbung

Realisierungsplanung



IP-Konzept

- IP-Adressbereiche & IP-Adressen
- Bildung von IP-Netzen
- Reservierung der Adressräume

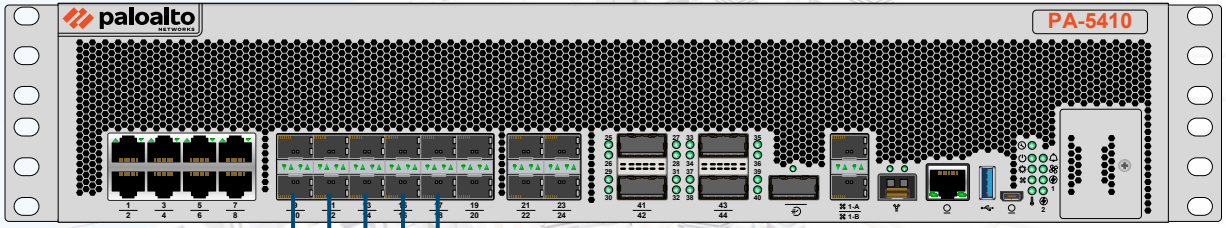
Netzdesgin

Segmer

ozesse

Werbung

Realisierungsplanung



Netzdesgin

Segmente

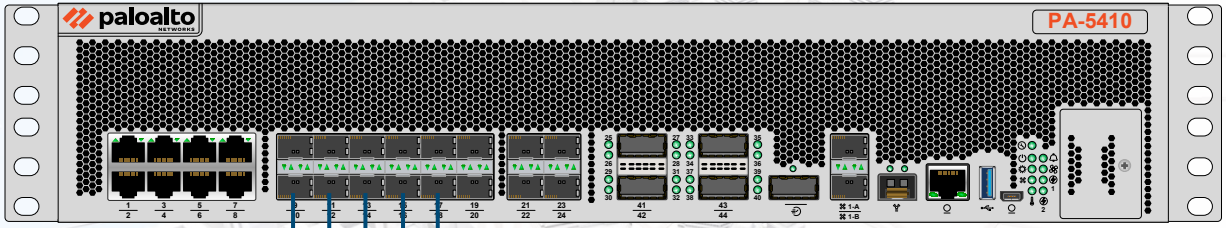
IP-Konzep

ung

Prozesse

- Anlage & Löschen neuer Freigaben
- Überprüfen von Freigaben
- Anlage & Löschen neuer Segmente
- Change-Management

Realisierungsplanung



Netzdesgin

IP-Konzept

Werbung

- Administratoren
- Anwender
- Management

1 Der große Traum

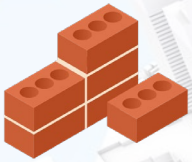
2 Die Bedarfsplanung

3 Die Realisierungsplanung

4 Die Umsetzung

Wie starte ich mit der Umsetzung?

Was ich habe…



…Skills…

Was ich möchte…

Understanding Security Zones

Security Zones sind eine logische Möglichkeit, physische und virtuelle Schnittstellen auf der Firewall zu gruppieren, um den Datenverkehr zu steuern und zu protokollieren, der bestimmte Schnittstellen in ihrem Netzwerk durchquert.

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-zones/security-zone-overview

Technische Umsetzung

Ein Beispiel…

Zone: Clients

Interfacekonfiguration

INTERFACE	TAG	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
ae1	Untagged		none	none	none	QoS	downlink internal network
ae1.11	11		192.168.11.1/24	default	Clients	IP DNS	Clients

(Security) Policy

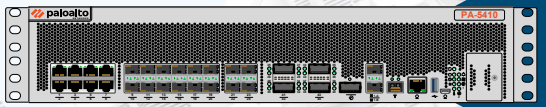
	Source			Destination			
ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE
Clients	PH_N_10.22.15.0-24	ho...	Clients	192.168.11.2	ssh	TCP_22
VPN		tim	Management	PH_H_Authentication_Proxy	ssl	TCP_443
IPSec			Proxy	PH_N_192.168.6.0-24		

Logging

FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	IP PROTOCOL	EGRESS I/F
Clients	Server	192.168.11.23		192.168.4.2	6690	tcp	ethernet1/7
Clients	DNS	10.22.10.23		198.18.0.1	53	udp	loopback.1

Technische Umsetzung

Wie viele Zonen braucht es?



Clients

Server

MGMT

Untrust

WiFi Clients

Server-SQL

Interne-IT

Testing

Printer

Deployment

Backup

INFRA-MGMT

DCs

Mobile

Handhelds

IPSec

Mail

Server-Apps

SRV-MGMT

VoIP

DMZ

VPN

CCTV

DoorAccess

SmartDevices

Technische Umsetzung

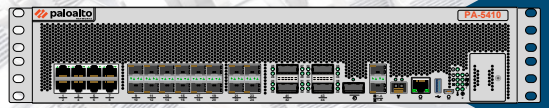
- Sortierung der Zonen in die Kategorien
- Verbesserung der Übersichtlichkeit
- Anpassung der Benamung möglich

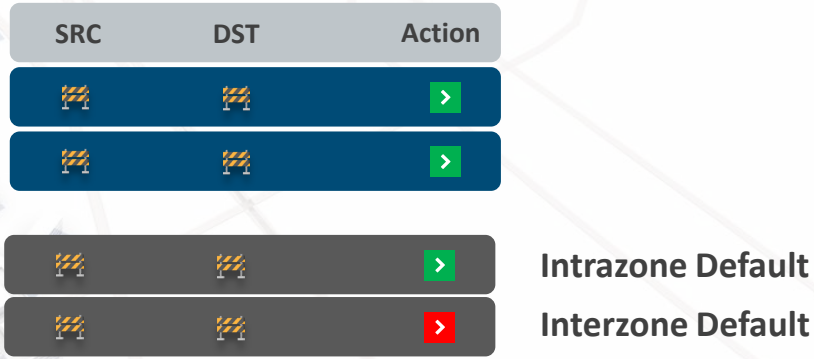
Technische Umsetzung

Intrazone Default

Interzone Default

Regelwerk



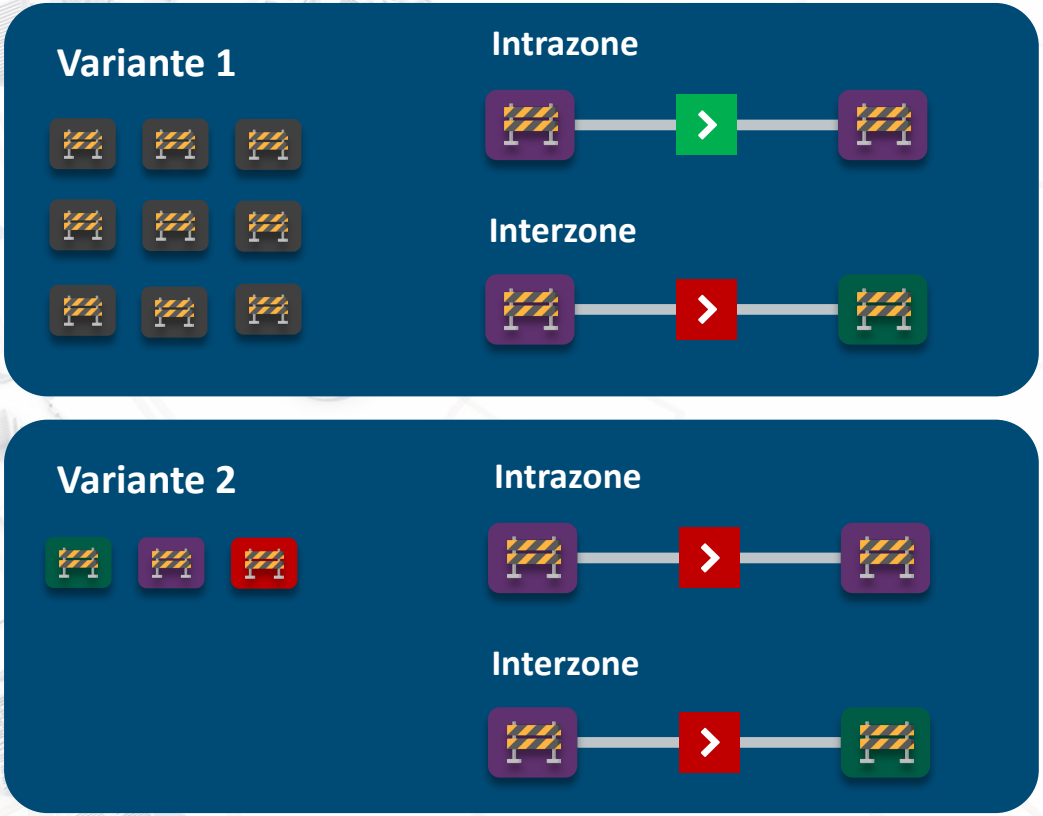


Technische Umsetzung

- Zwei Möglichkeiten zum Aufbau der Zonen/des Regelwerks

Unterschiede in:

- Anzahl der Zonen
- Komplexität der Regeln
- Bereitstellung von Services



- Bereitstellung von Services am Beispiel von DHCP

Variante 1

Intrazone

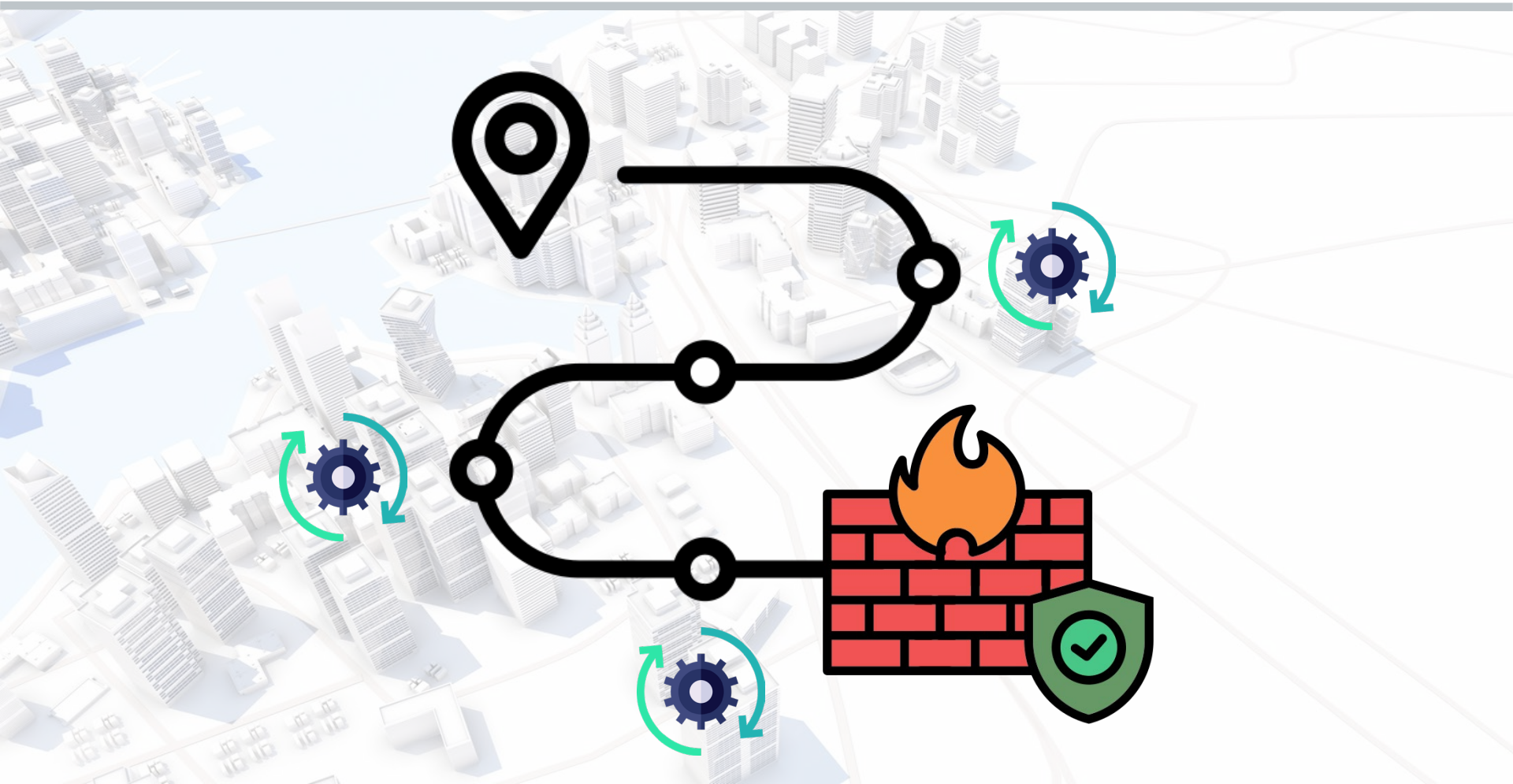
Variante 2

Intrazone

Organisatorische Grundlagen schaffen

- Integration in die Organisation
- Prozesse anpassen
- Das Zielbild kommunizieren
- Migrationsplanung erstellen?!?

Integrierte Migration



Integrierte Migration

Netz anlegen

System umziehen

Kommunikation monitoren

Regeln aktivieren

Clients

Server

Server- Apps

DCs

MGMT

INFRA- MGMT

SRV- MGMT

Untrust

IPSec

DMZ

Integrierte Migration

Integrierte Migration

Netz anlegen

System umziehen

Kommunikation monitoren

Regeln aktivieren

Integrierte Migration

Integrierte Migration

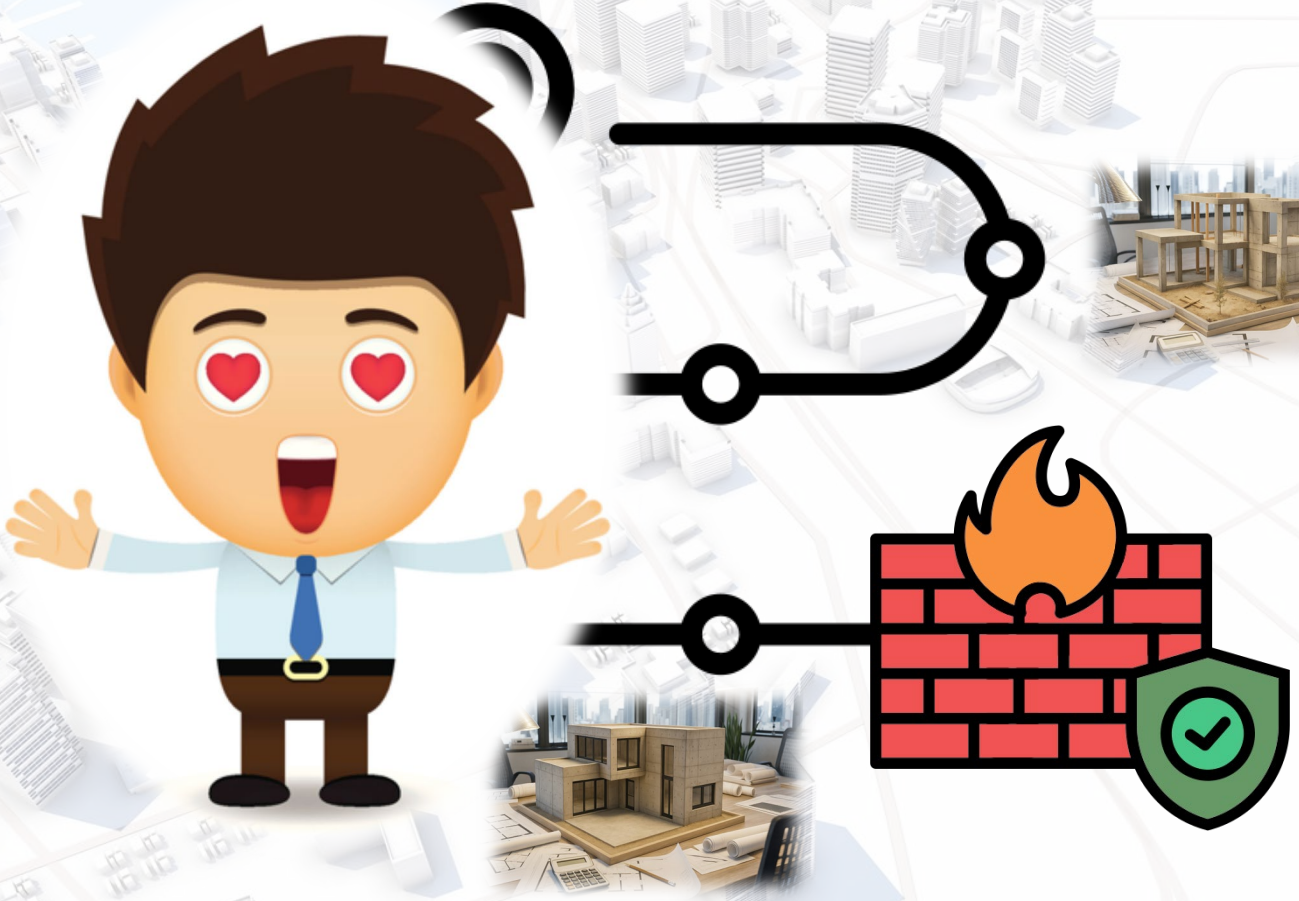
Netz anlegen

System umziehen

Kommunikation monitoren

Regeln aktivieren

Integrierte Migration



Der Traum ist erfüllt

- Integriere die Segmentierung in bestehende Strukturen
- Etabliere ein System, dass sich selbst pflegt und bereinigt
- Nähere dich inkrementell dem Ziel – Segmentierung ist kein Big Bang

Connected?

Alexander Vogt

Daniel Rehnitz

Tim Klotzbach

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.