

SD-LAN

Nice to have oder lukrativer Business Case?

Telekom Solution X

27.04.2023 – Frankfurt am Main



ERLEBEN, WAS VERBINDET.

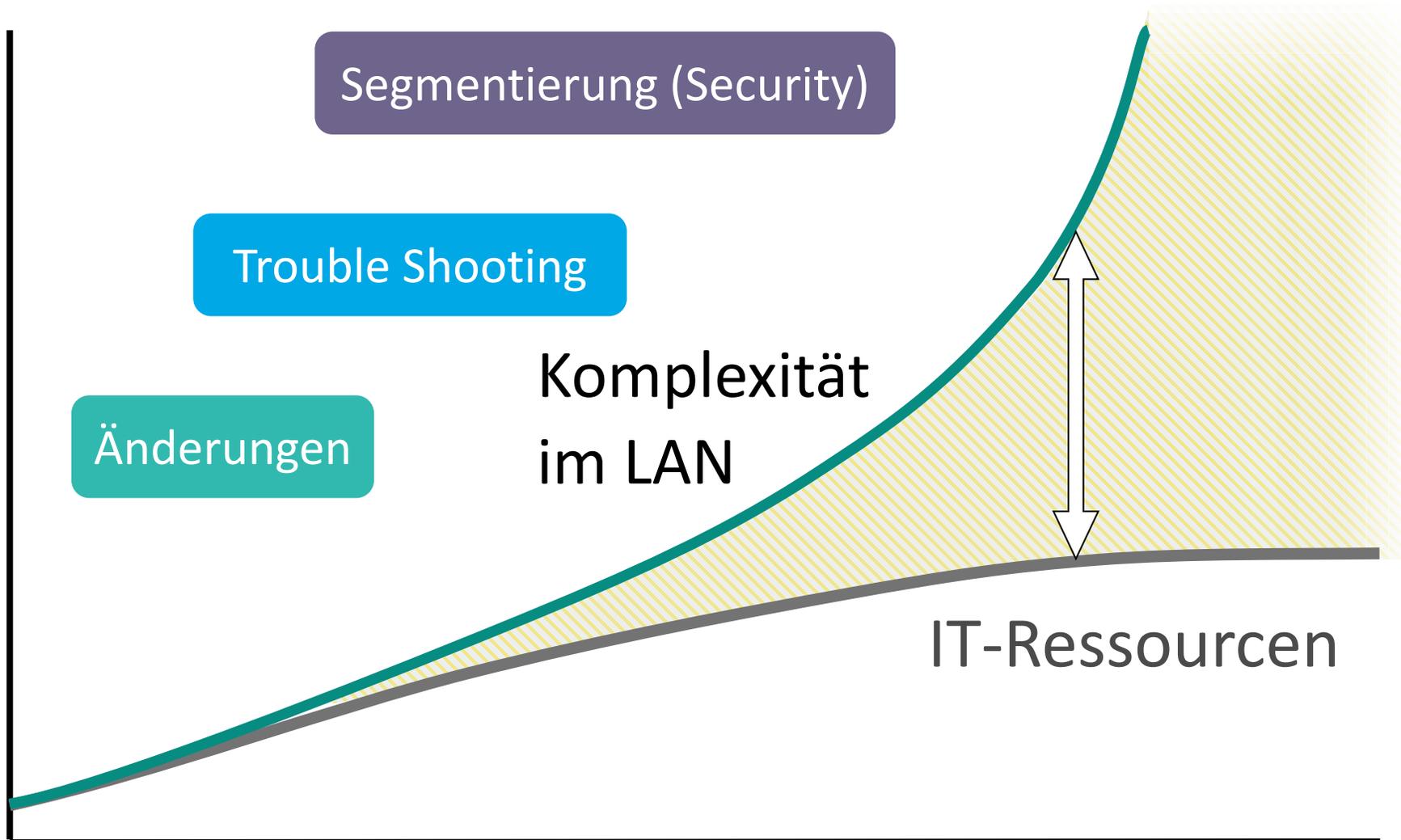


Agenda



- Warum?
- Was?
- Wie?
- Wofür?
- Wieviel?

Warum SD-LAN



**MITARBEITER
GESUCHT**



**MITARBEITER
GESUCHT**

Hören Sie auf, sich um Dinge zu kümmern,
die Maschinen schneller und besser können.

Die Krux im traditionellen LAN

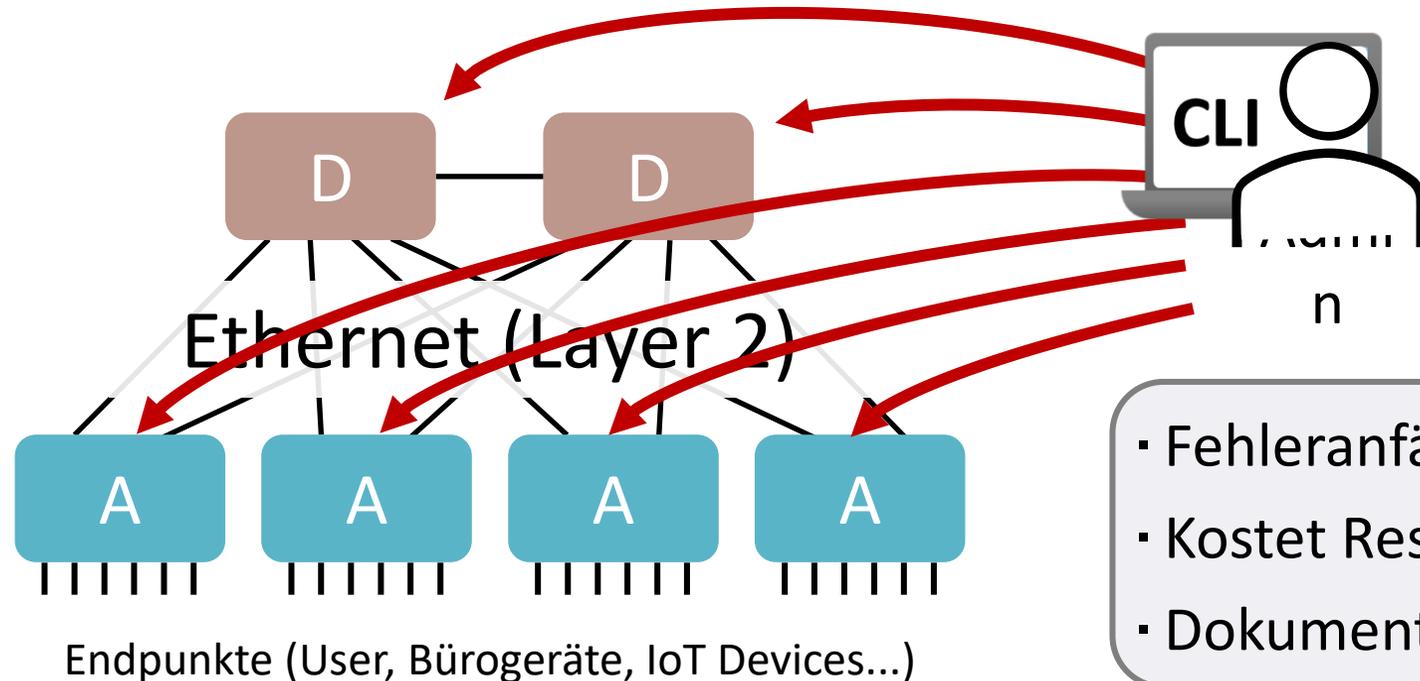
Änderungen

Trouble Shooting

Segmentierung (Security)

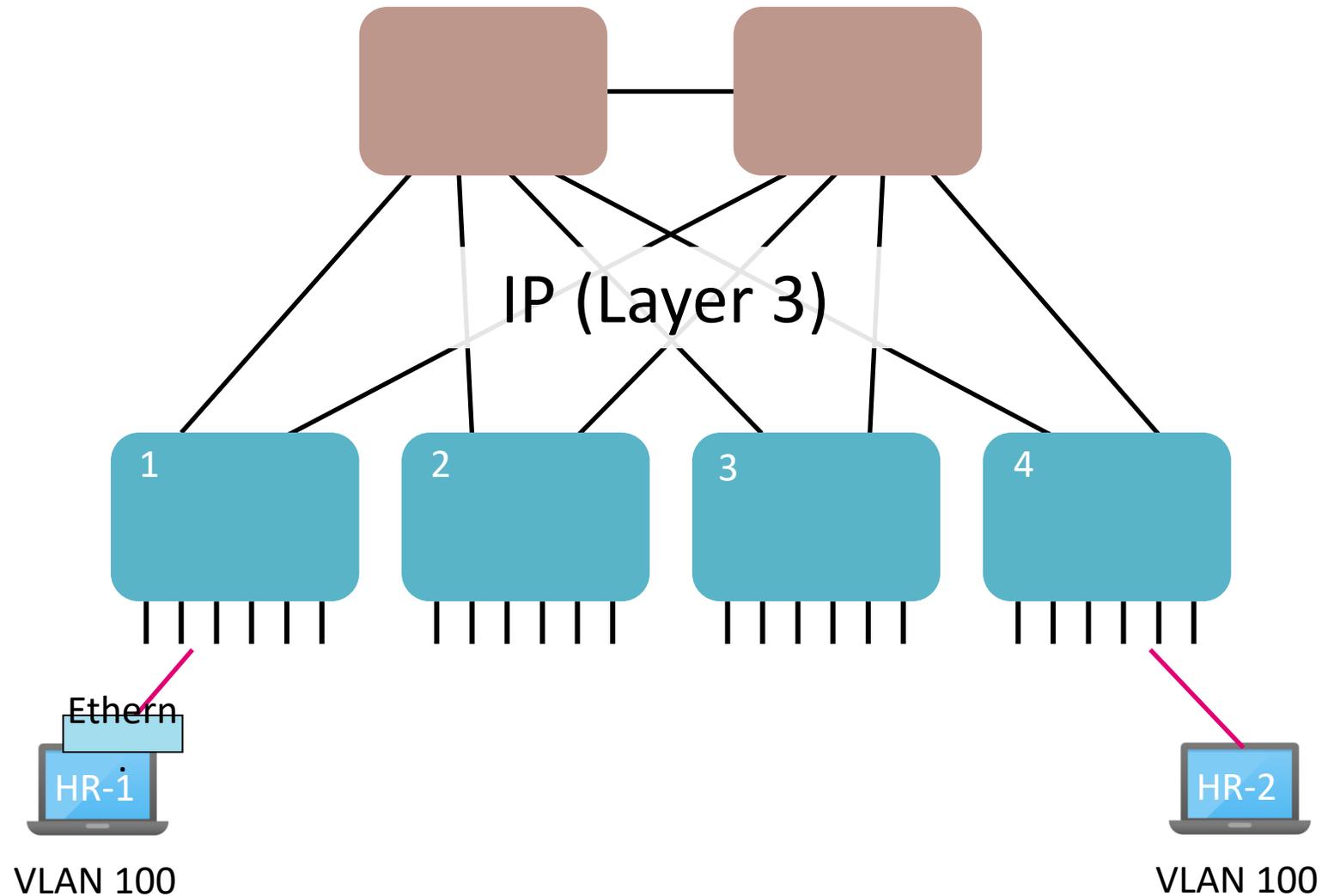
Security } -Policies
QoS }

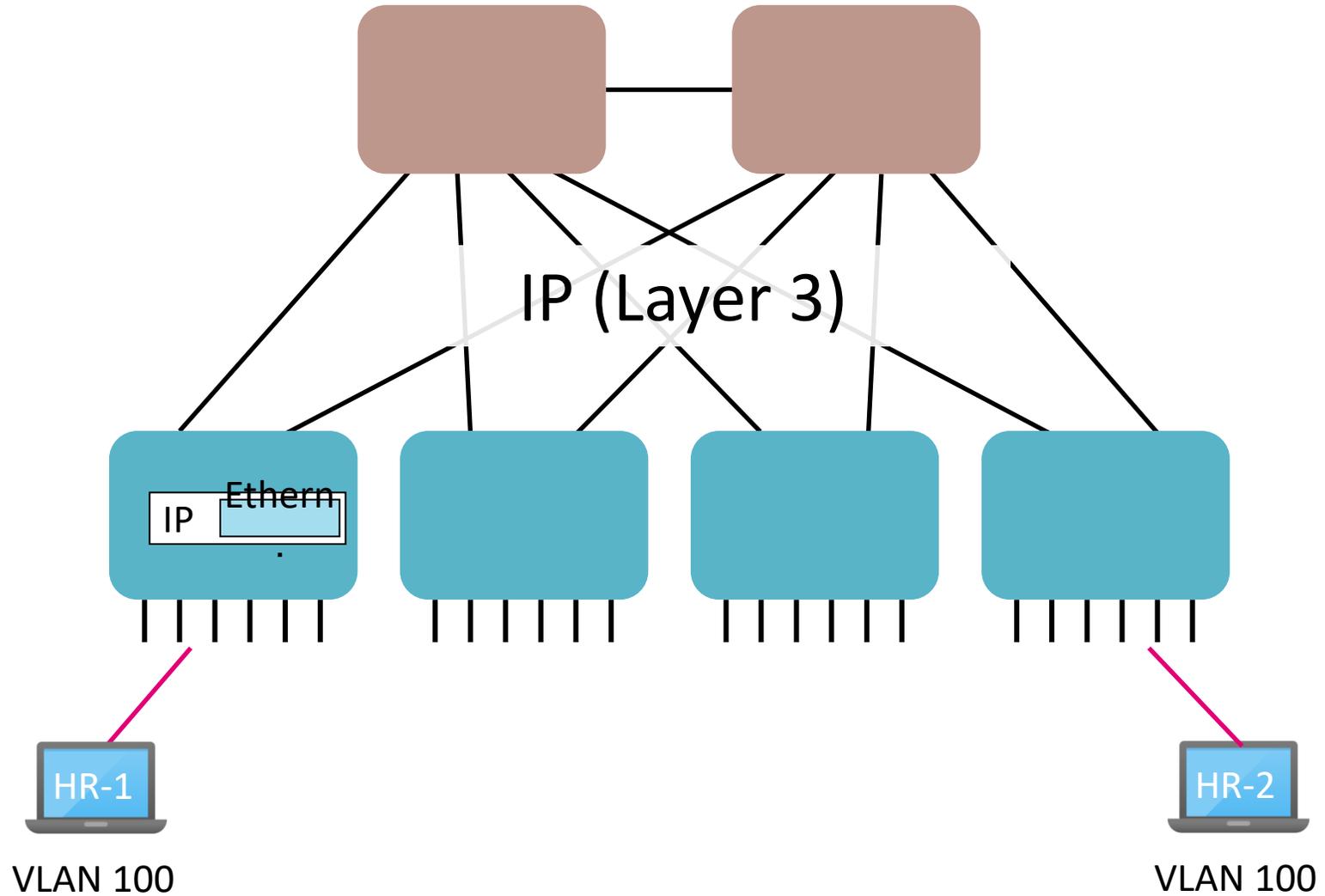
→ VLANs (Layer 2)

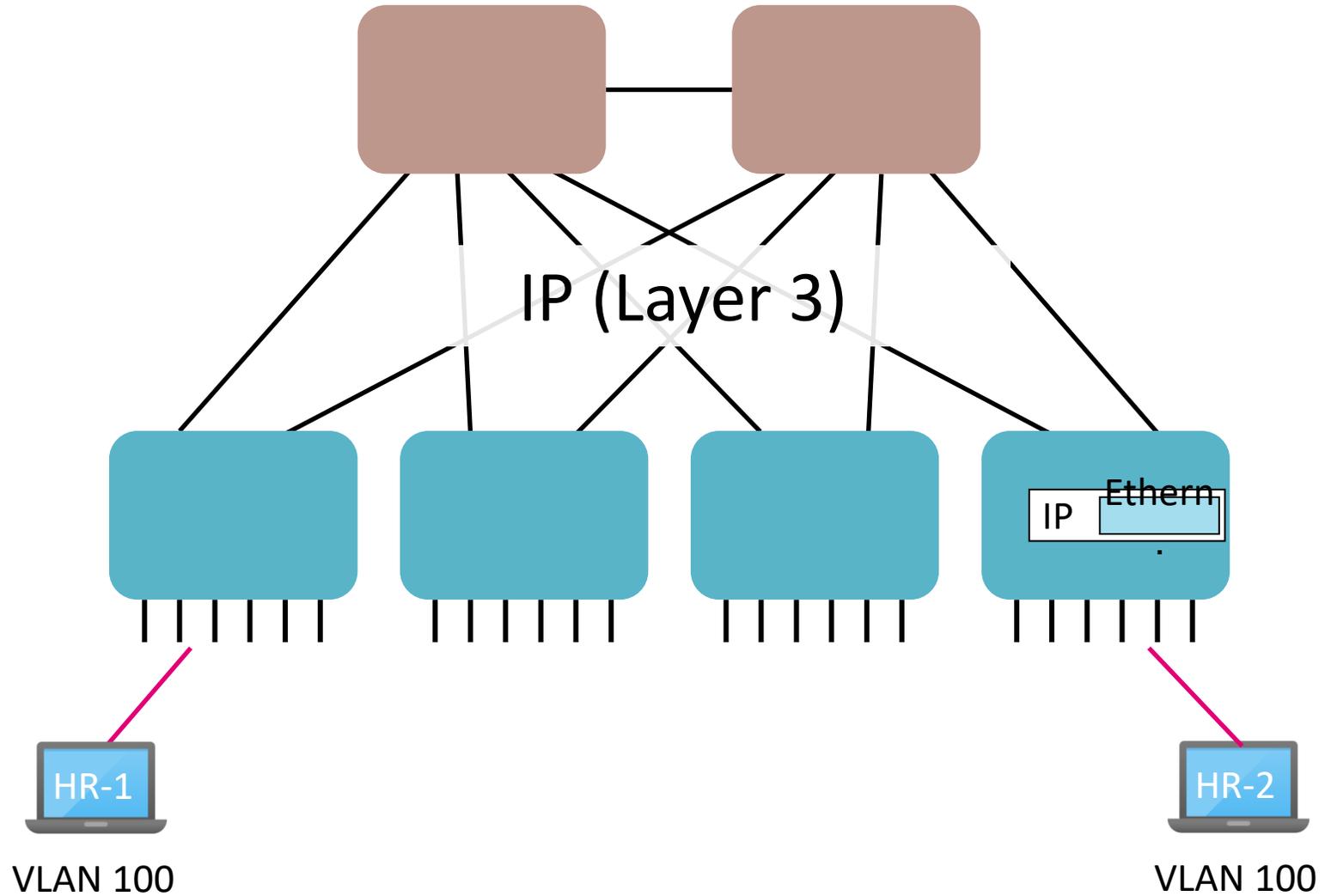


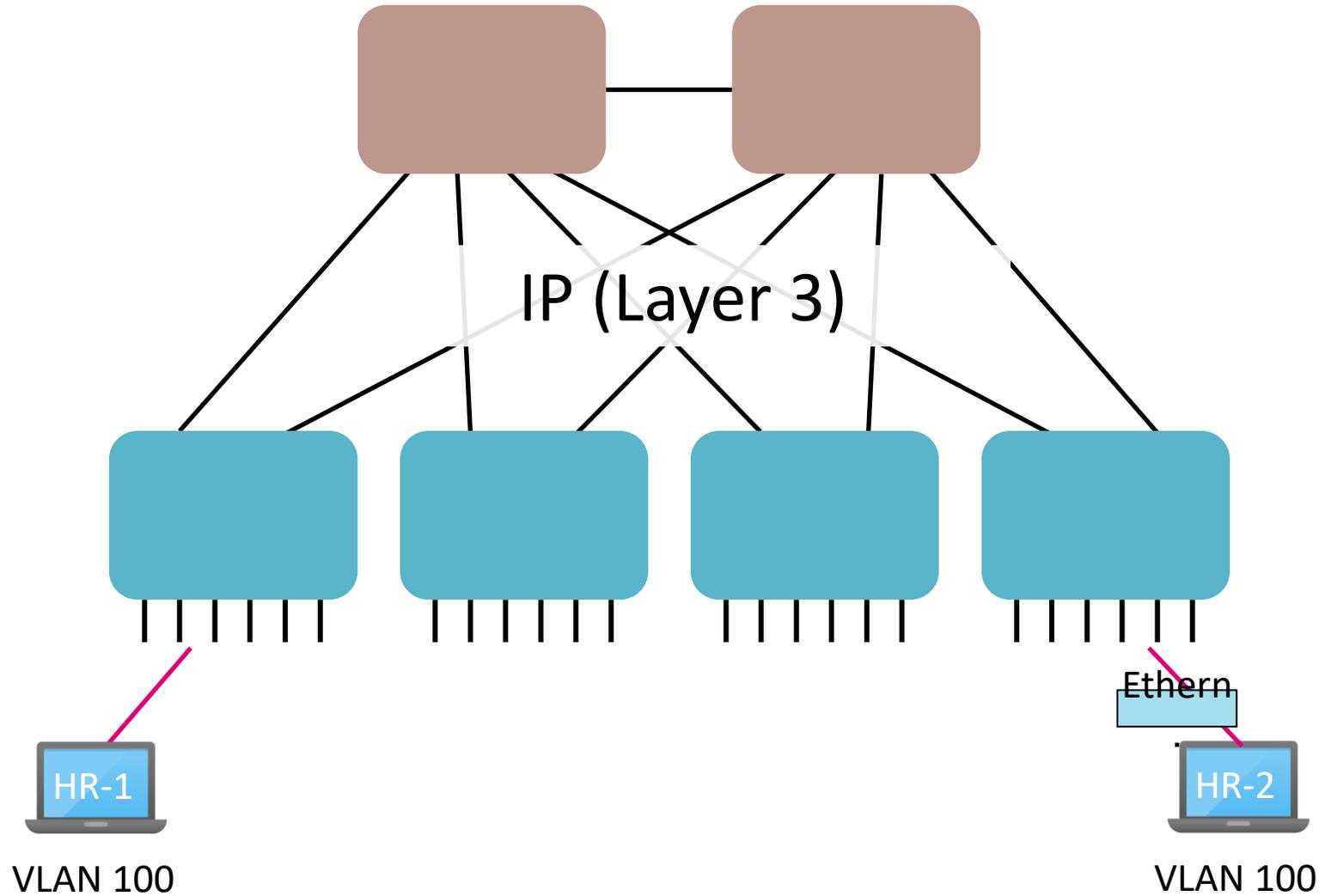
- Fehleranfällig
- Kostet Ressourcen
- Dokumentation?

How to define LAN via Software?

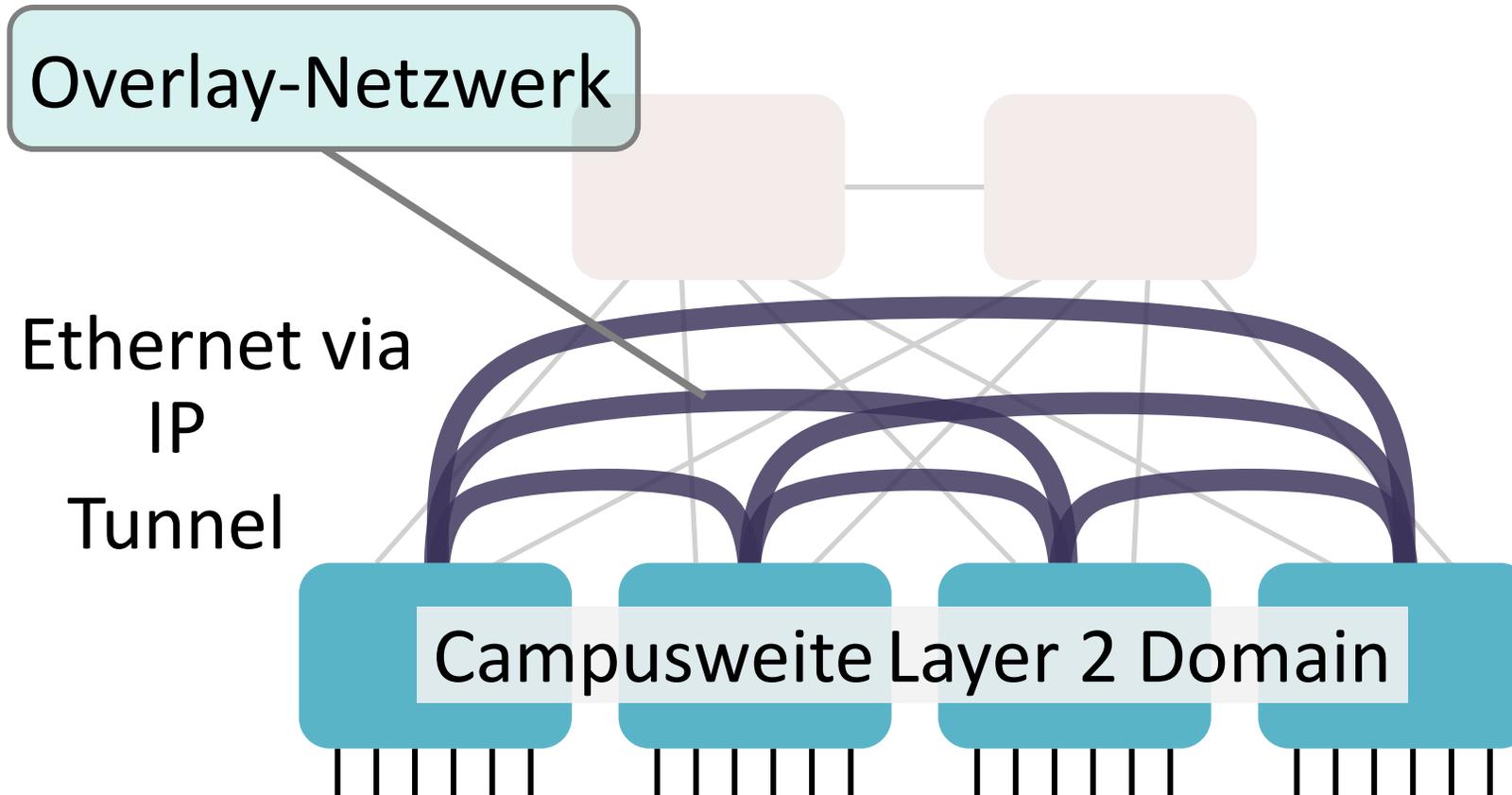




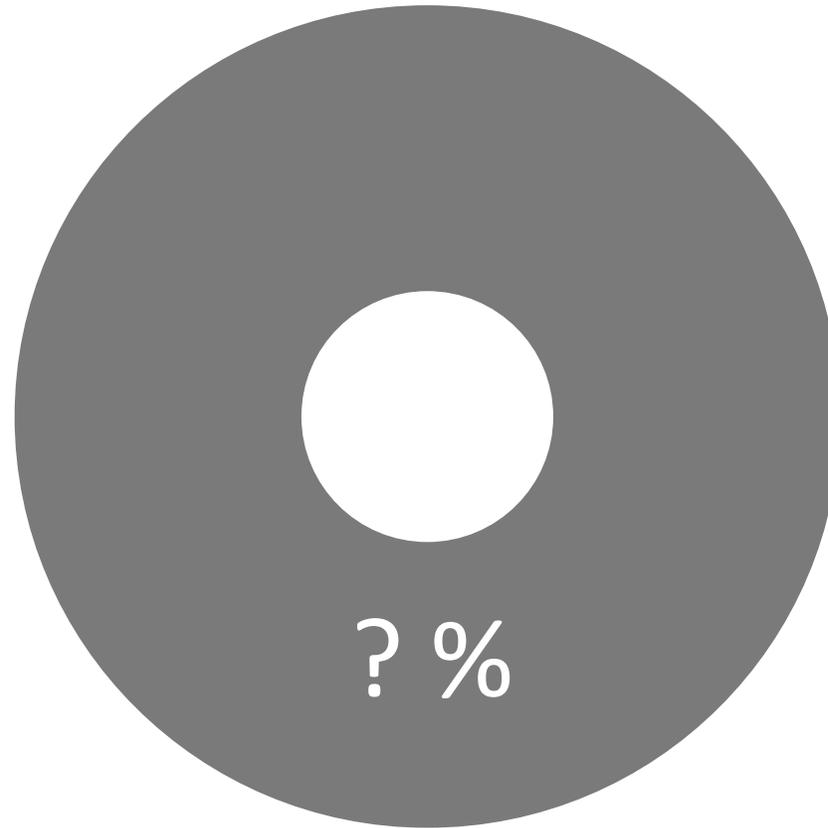




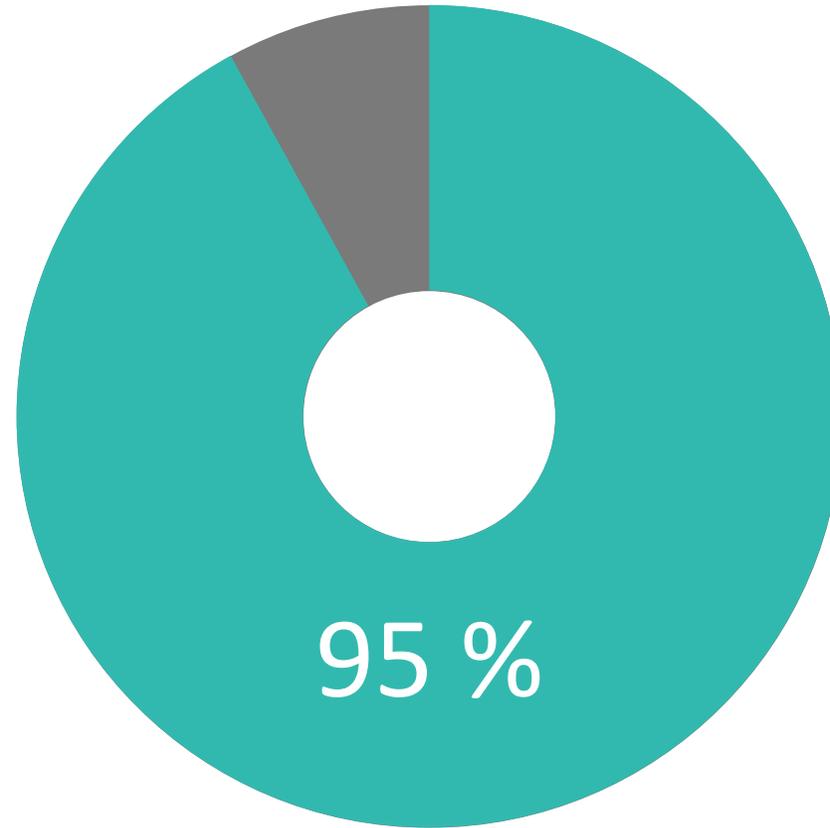
Logisches Overlay - Physisches Underlay



- Änderungs-resilientes Netzwerk
- Keine VLANs mehr nötig
- Extensiv skalierbares LAN

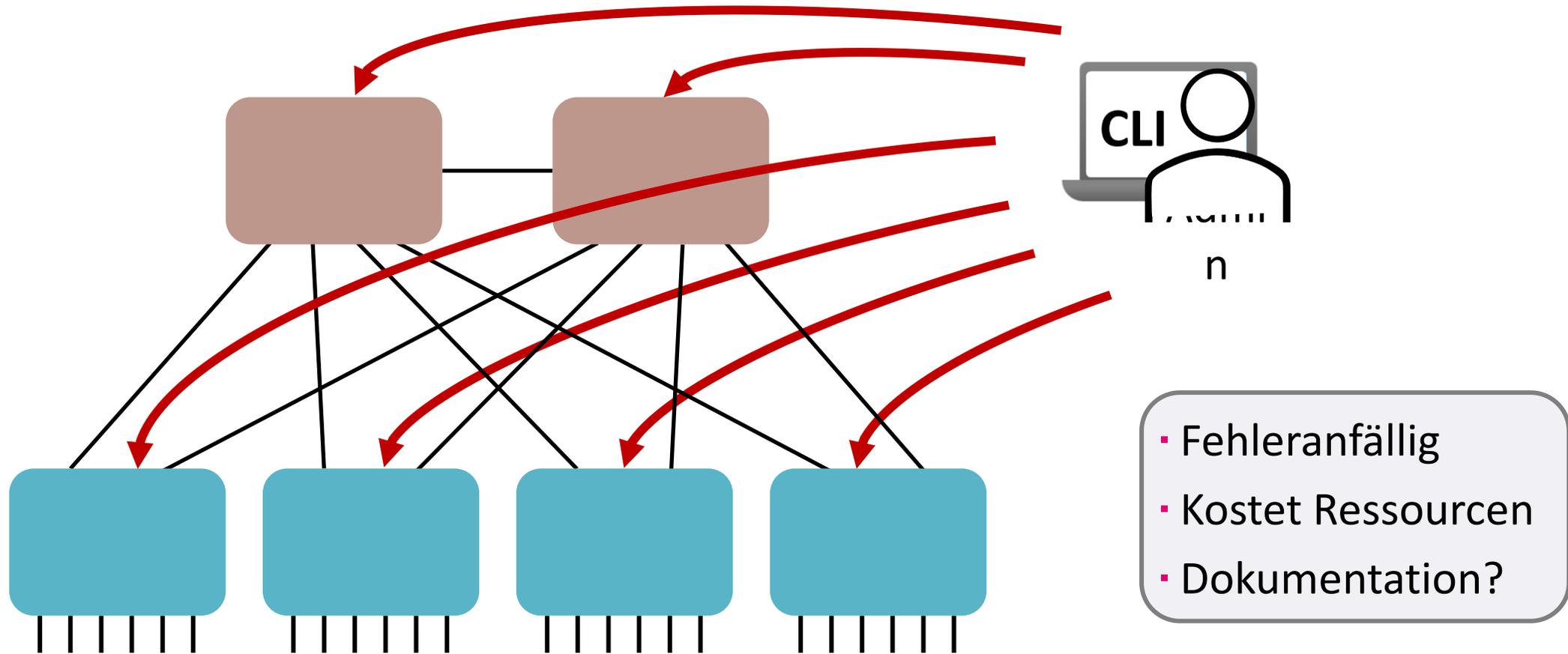


...aller Änderungen am Netzwerk erfolgen manuell

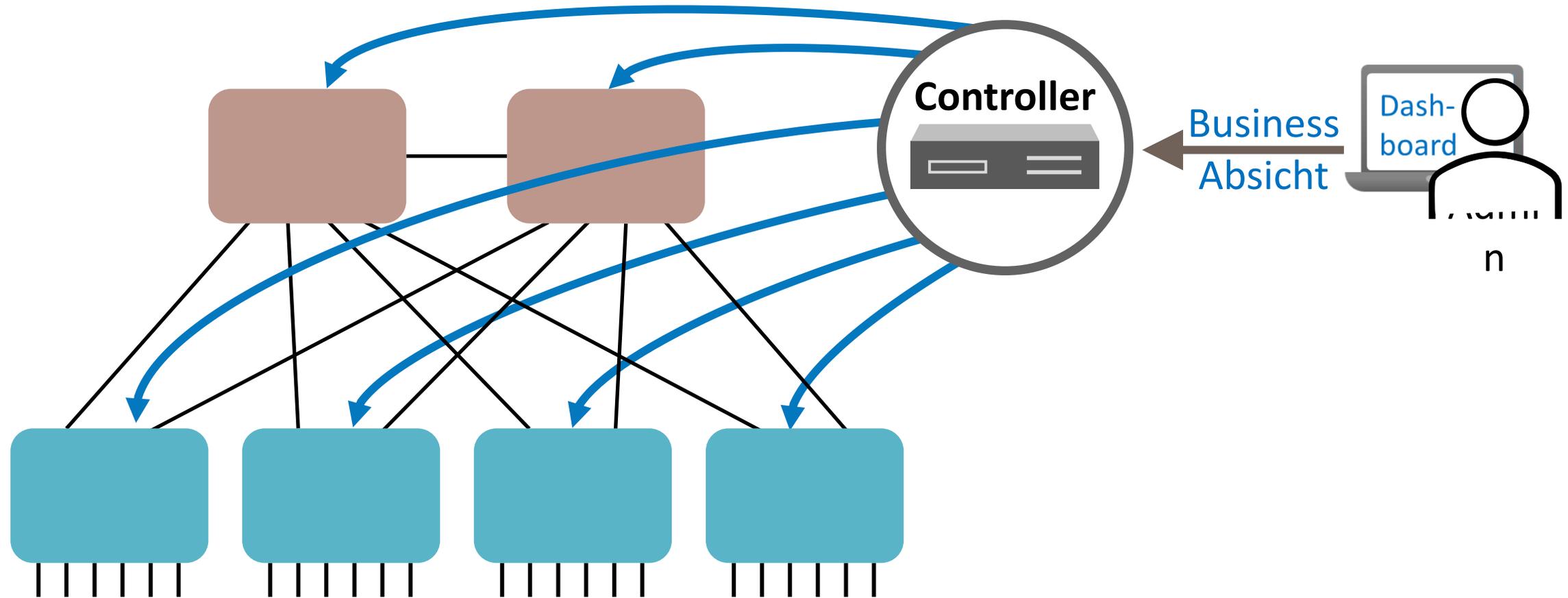


...aller Änderungen am Netzwerk erfolgen manuell

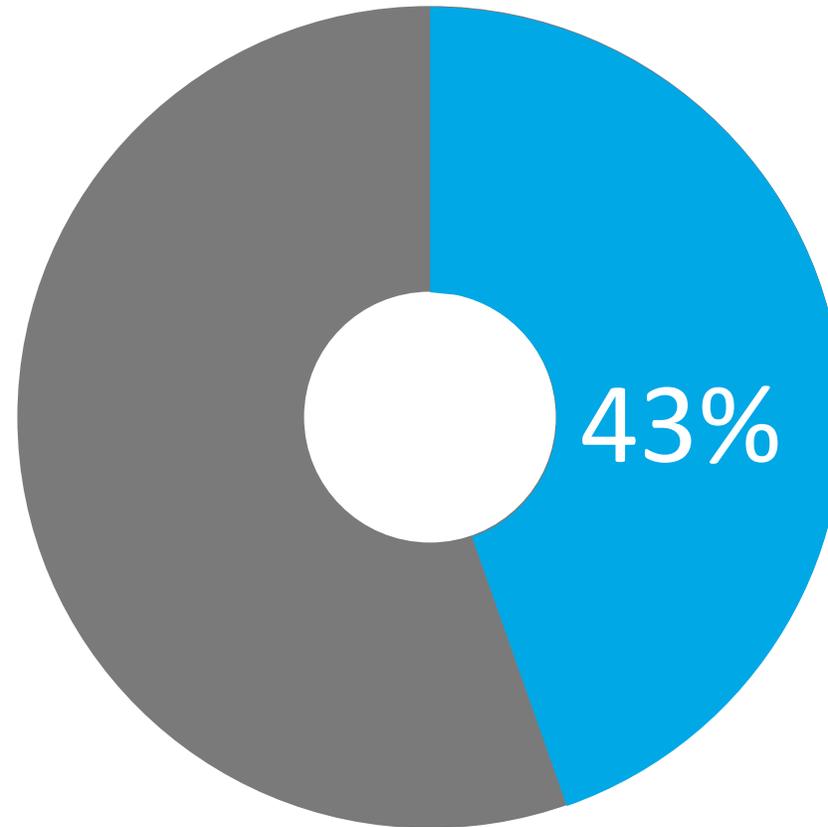
Von 95% Handarbeit...



...zum Intent Based Networking

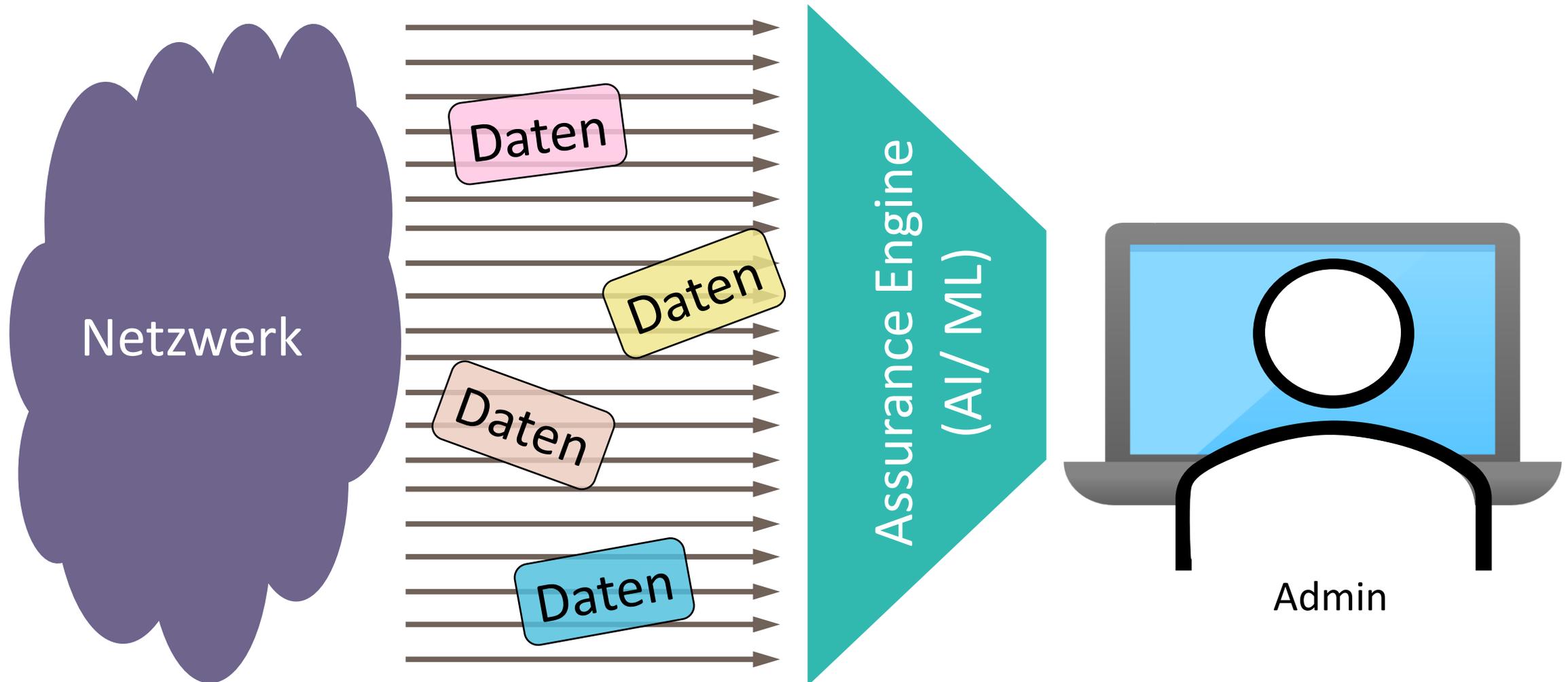


Troubleshooting & Assurance

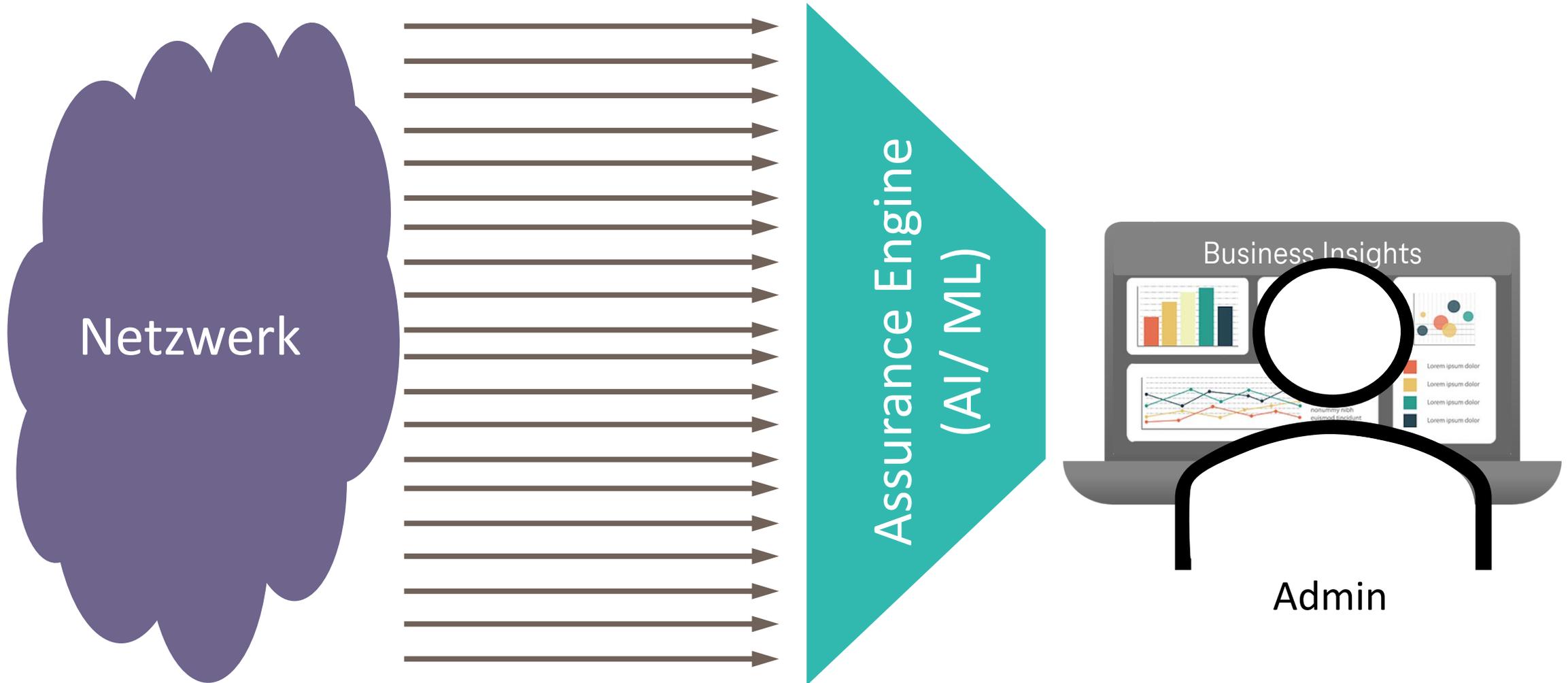


...der IT Ressourcen gehen für Troubleshooting drauf

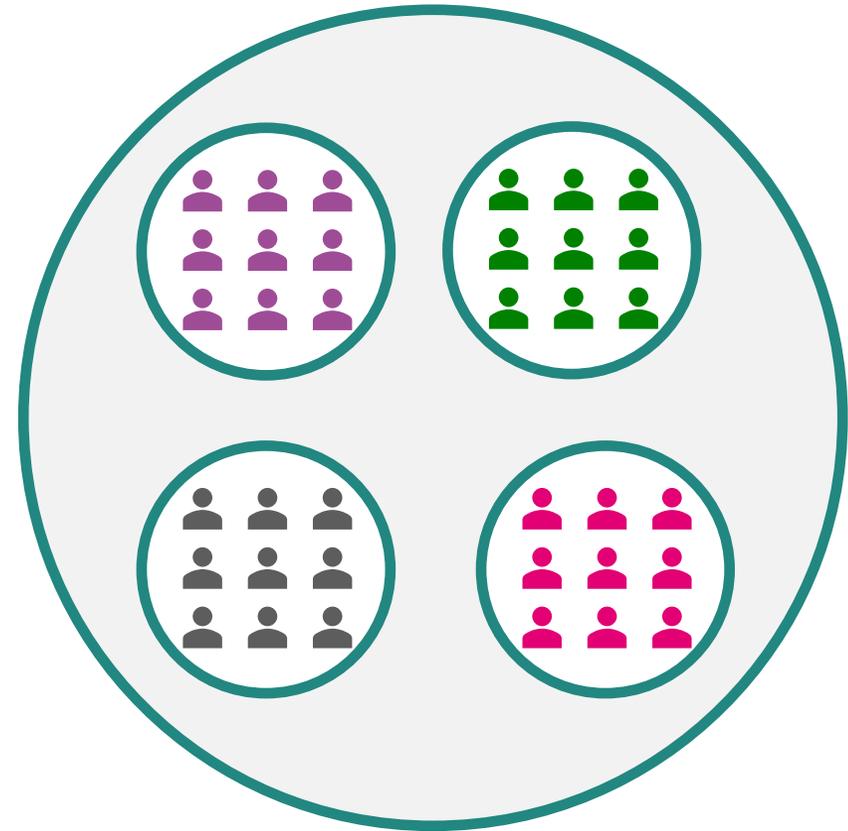
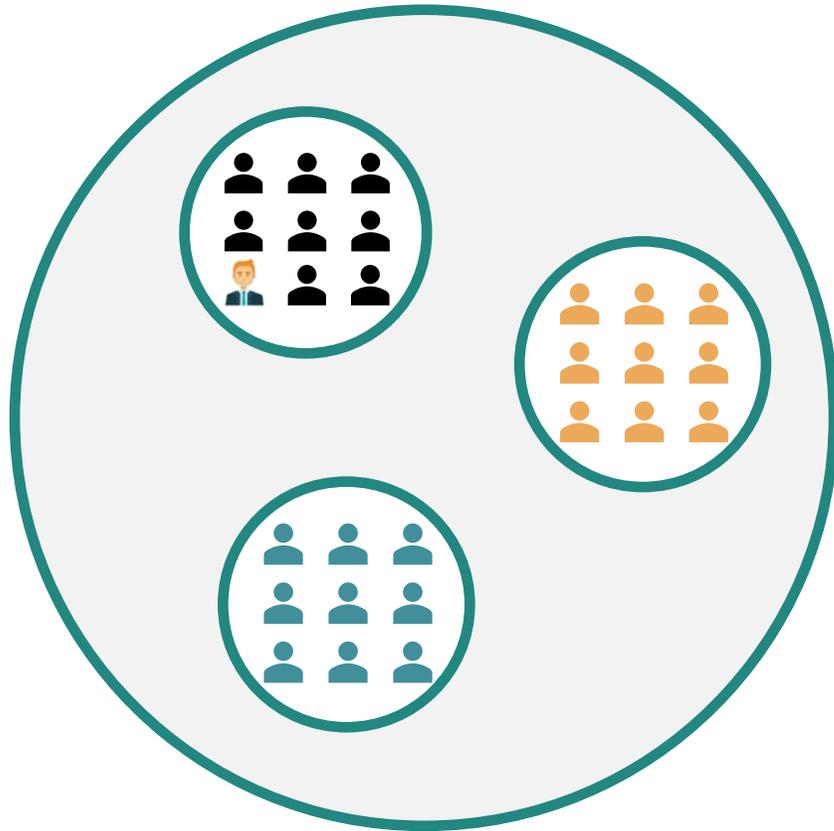
Troubleshooting & Assurance



Troubleshooting & Assurance

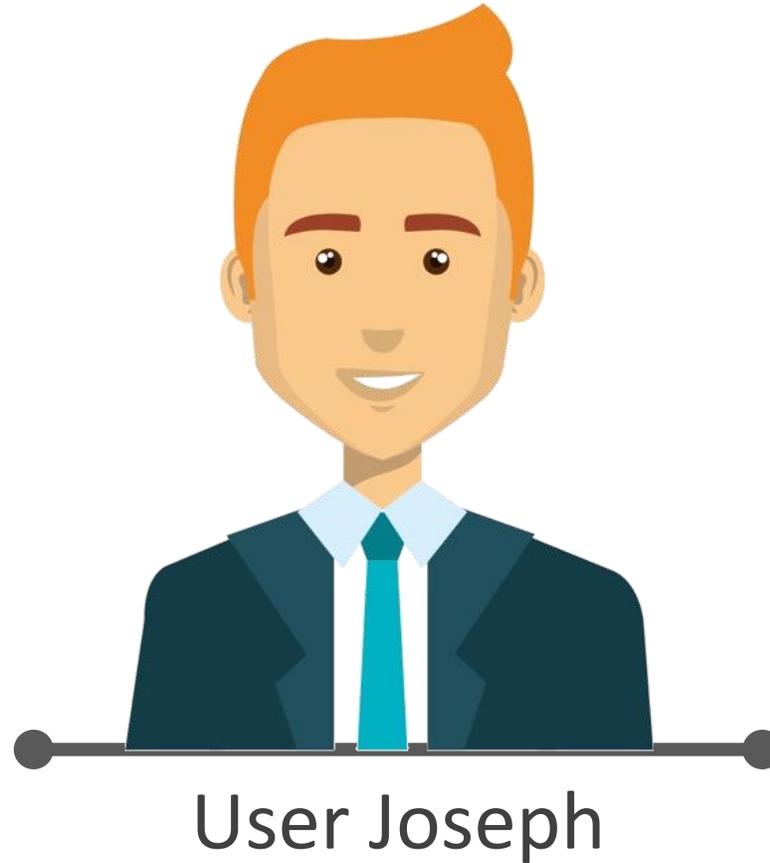


Makro- und Mikrosegmentierung ohne VLANs

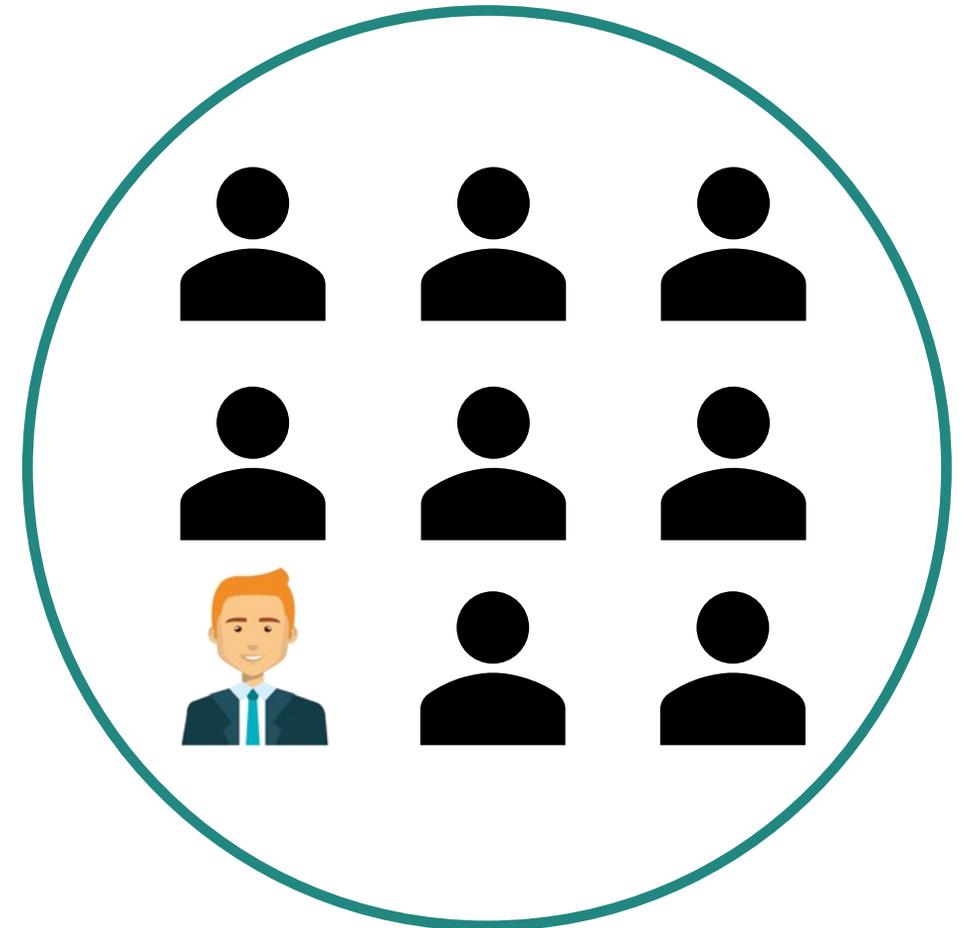
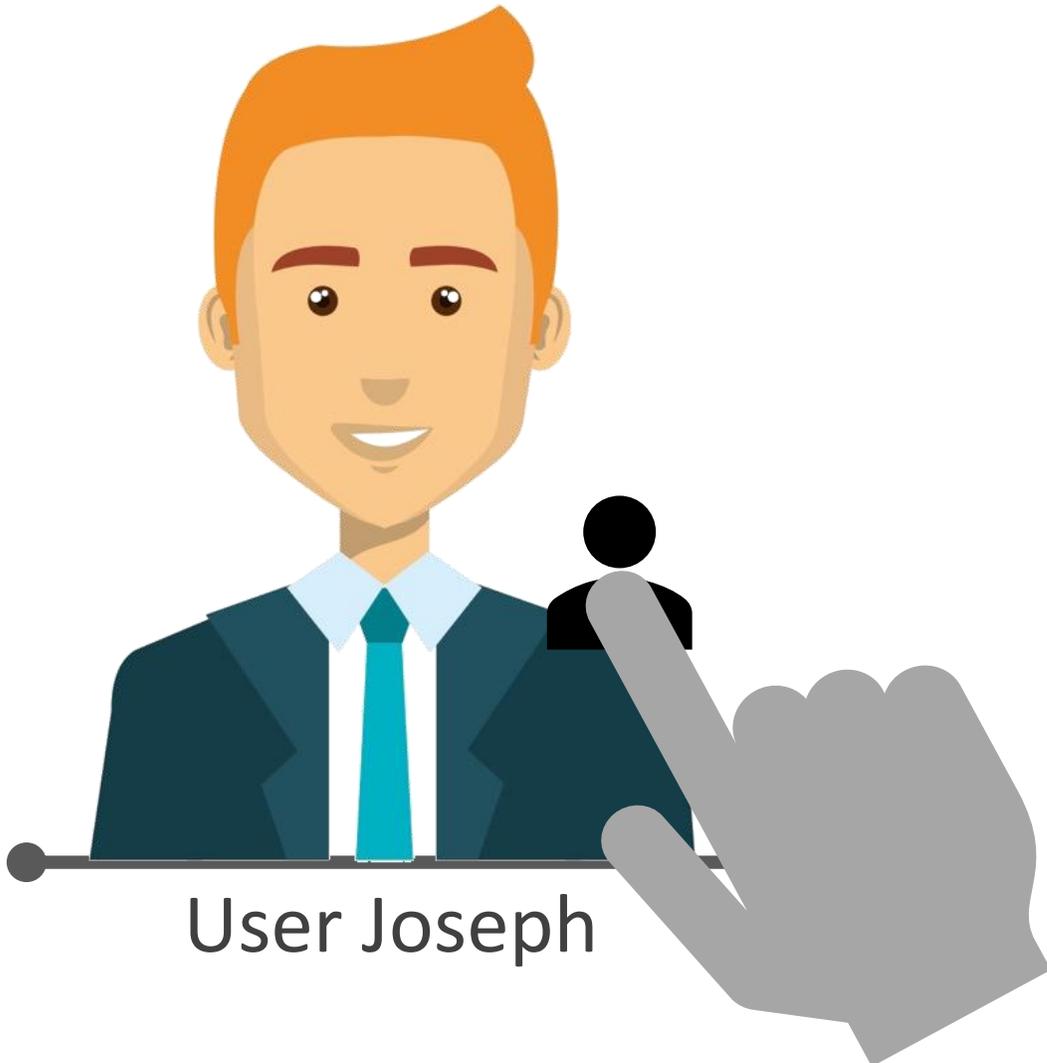


Es beginnt mit einem
User,

einem Device oder Thing



Wir ziehen den User in eine „Secure Group“ (SG)

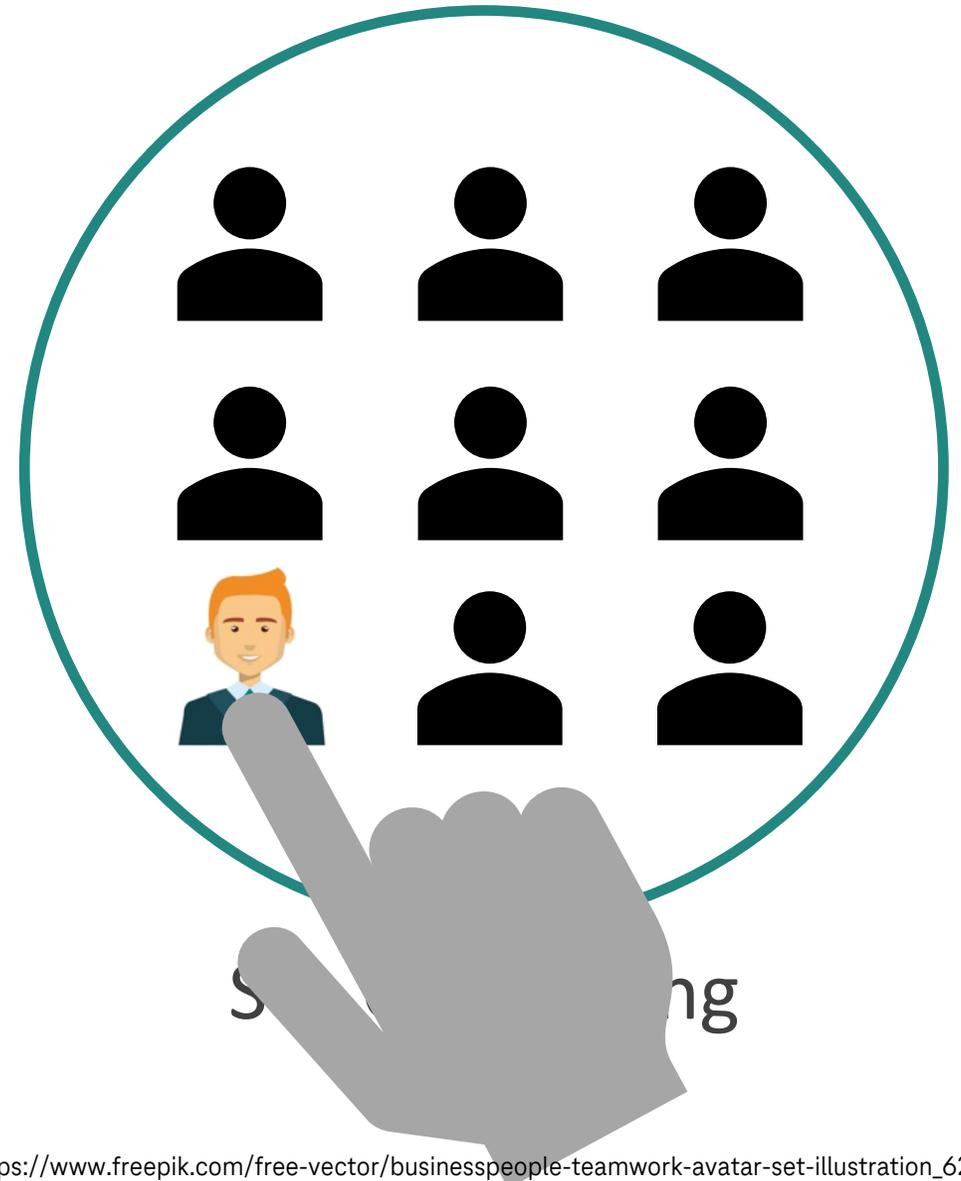


SG: Controlling

Wir ziehen den User in eine „Secure Group“ (SG)



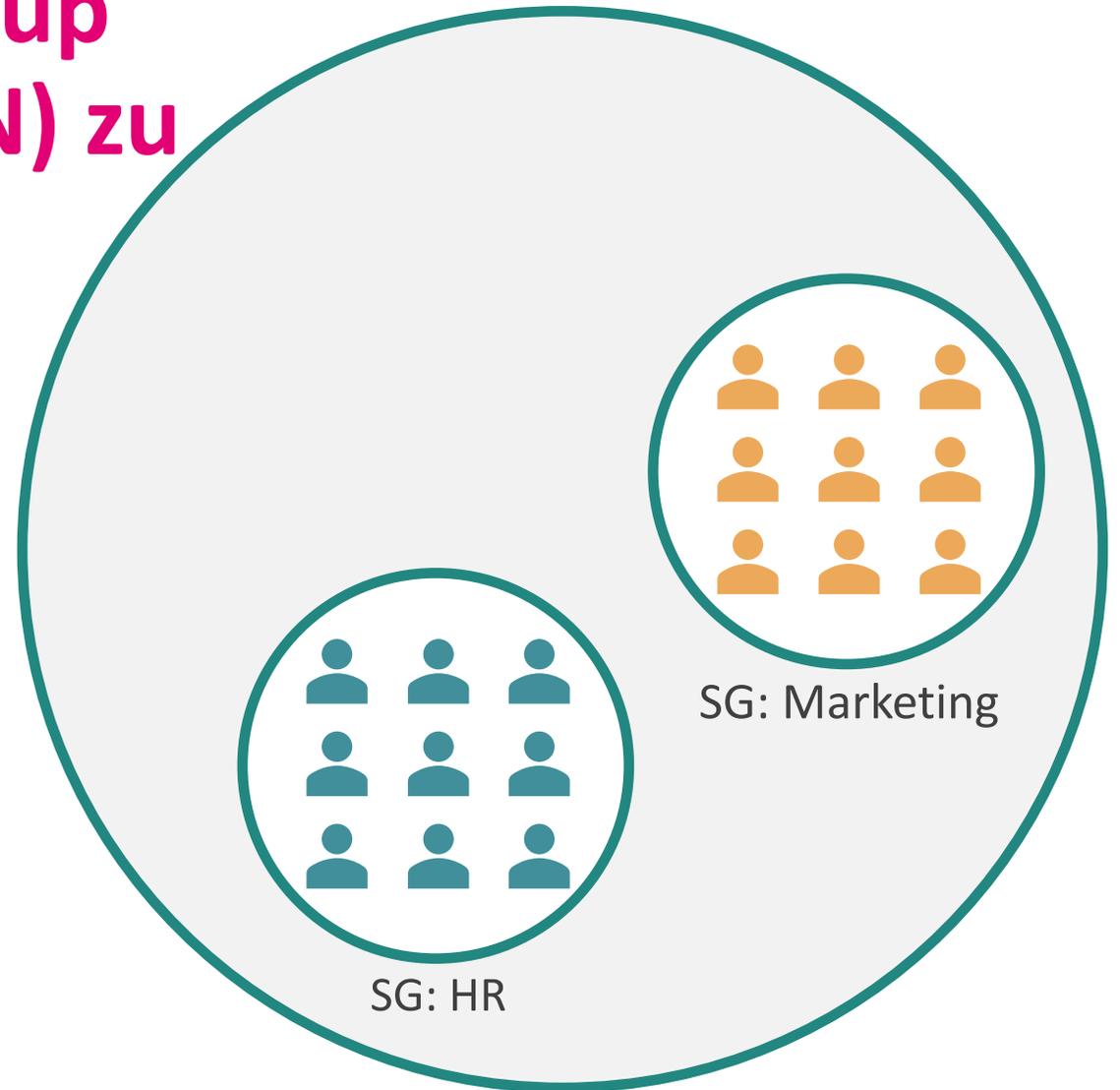
User Joseph



Wir ordnen die Secure Group einem Virtual Network (VN) zu



SG: Consulting

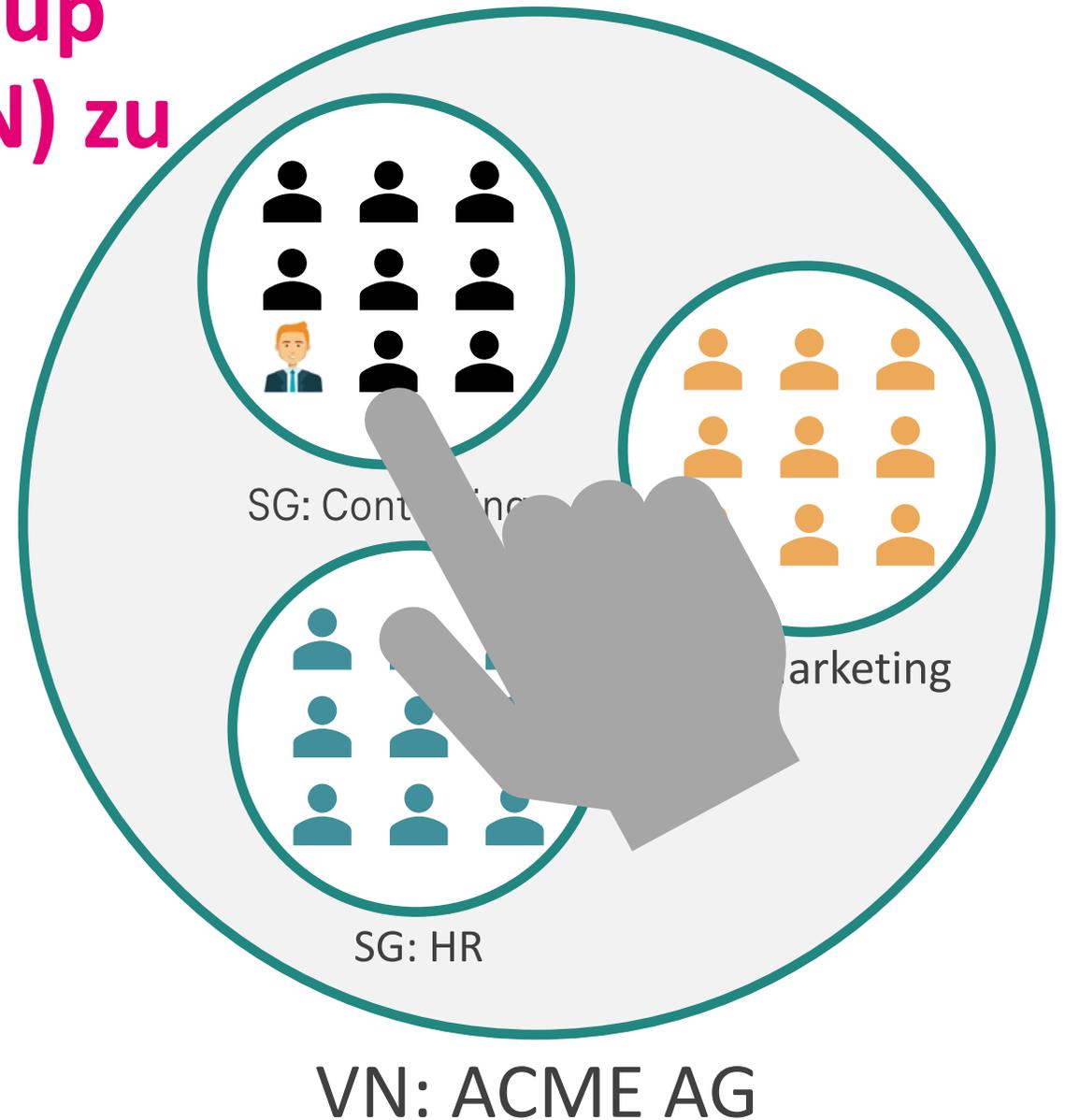


SG: HR

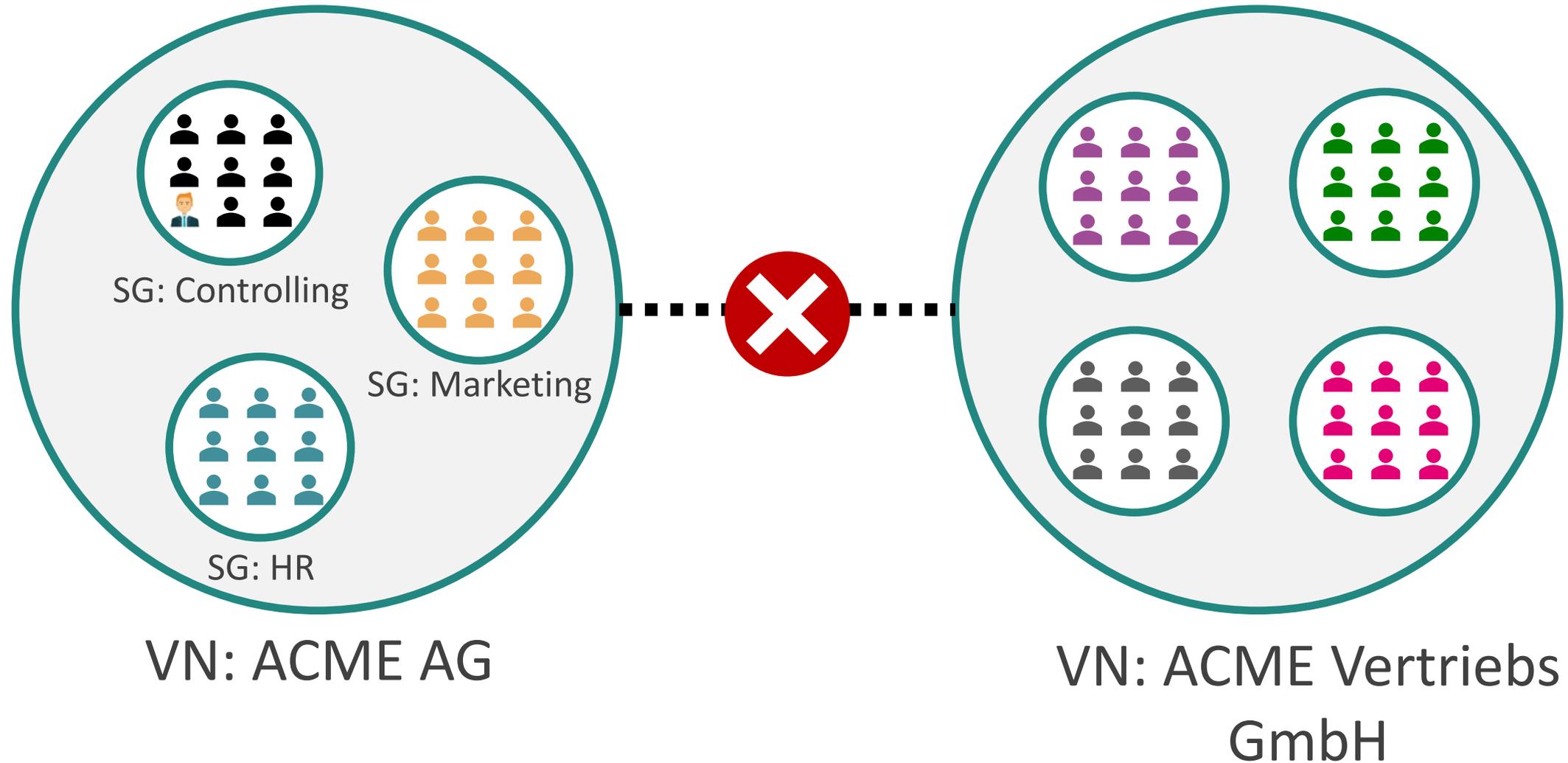
SG: Marketing

VN: ACME AG

Wir ordnen die Secure Group einem Virtual Network (VN) zu

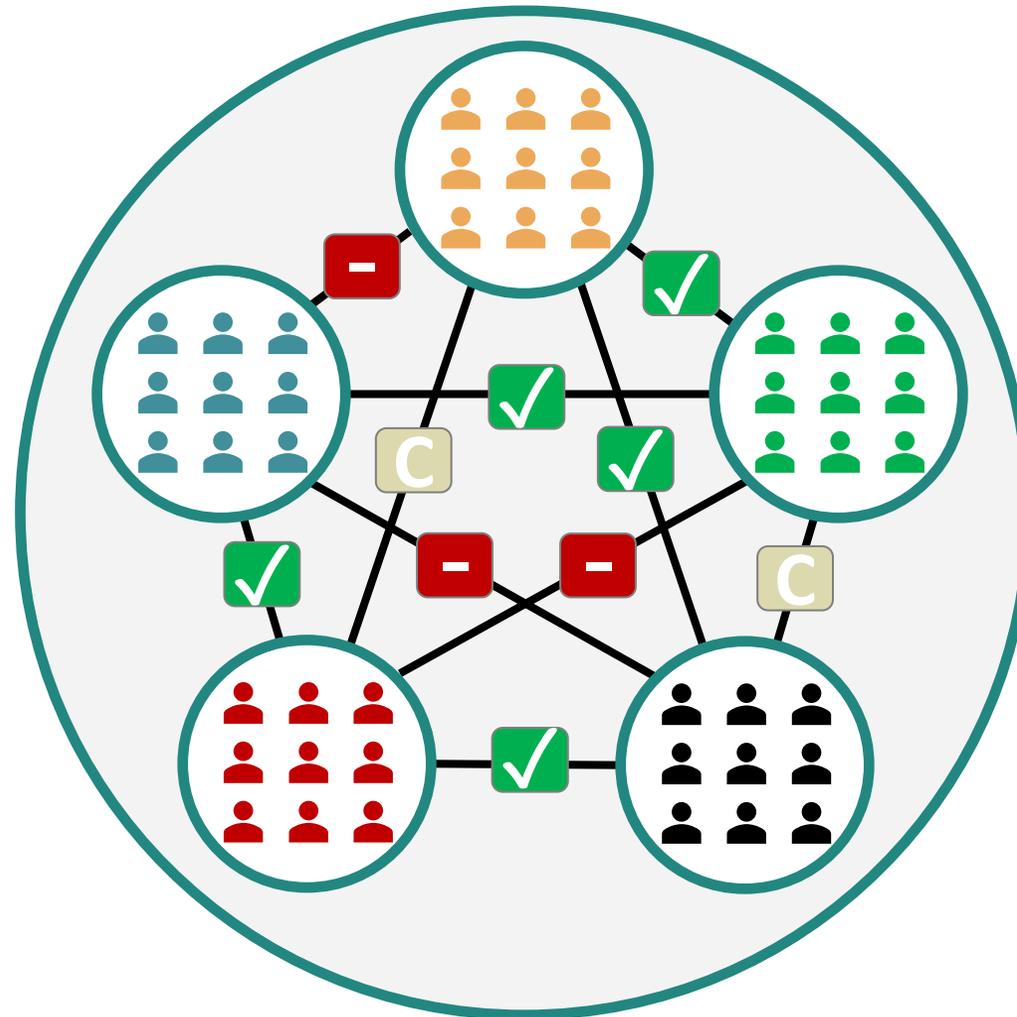


Makro-Segmentierung → Zwischen Netzwerken



Mikro-Segmentierung → Innerhalb eines Netzwerks

-  Deny
-  Permit
-  Custom



Virtual Network A

Policies (106) [Exit full screen](#)

Filter | Deploy ▼ Refresh

■ Permit
 ■ Deny
 ■ Custom
 Default

Source	Auditors	Auditor_SDA	BYOD	Cameras	Contractor_Nur...	Contractors	Developers	Development_S...	Doctors	Employees	Finance_Server...	Guests	HVAC	Lights	Network_Serv...	PCI_Servers	Point_of_Sale...	Printer_EPG	Production_S...	Production_U...	Quarantined_...	TrustedDevices	Badge-Readers	UntrustedDevi...	TrustSec_Devi...	Unknown
Auditors	Deny	Permit	Custom	Permit	Permit	Custom	Custom	Permit	Permit	Custom	Default	Default	Default	Default	Default	Custom	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Auditor_SDA	Default	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Deny	Permit	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
BYOD	Deny	Permit	Custom	Permit	Deny	Custom	Deny	Permit	Permit	Custom	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Cameras	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Deny	Default	Default	Deny	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Contractor_Nur...	Deny	Deny	Permit	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Contractors	Deny	Deny	Custom	Deny	Deny	Custom	Custom	Permit	Permit	Custom	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Developers	Deny	Deny	Custom	Deny	Custom	Custom	Custom	Permit	Permit	Custom	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Development_S...	Deny	Deny	Deny	Deny	Deny	Custom	Permit	Permit	Deny	Permit	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Doctors	Permit	Permit	Permit	Permit	Permit	Custom	Permit	Permit	Deny	Permit	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Employees	Deny	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Default	Default	Deny	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Permit	Default
Finance_Server...	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
Guests	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Deny	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default
HVAC	Default	Default	Default	Deny	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default	Deny	Default	Default	Default	Default	Default	Default	Default	Default	Default	Default

Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

Policies (106) [Exit full screen](#)

Filter | Deploy | Refresh

■ Permit
 ■ Deny
 ■ Custom
 Default

Source	Auditors	Auditor_SDA	BYOD	Cameras	Contractor_Nur...	Contractors	Developers	Development_S...	Doctors	Employees	Finance_Server...	Guests	HVAC	Lights	Network_Serv...	PCI_Servers	Point_of_Sale...	Printer_EPG	Production_S...	Production_U...	Quarantined_...	TrustedDevices	Badge-Readers	UntrustedDevi...	TrustSec_Devi...	Unknow
Auditors	Deny	Permit	Custom	Permit	Permit	Custom	Custom	Permit	Permit	Custom																
Auditor_SDA		Deny	Permit	Permit	Permit	Permit	Permit	Permit	Deny	Permit																
BYOD	Deny	Permit	Custom	Permit	Deny	Custom	Deny	Permit	Permit	Custom																
Cameras	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Deny			Deny													
Contractor_Nur...	Deny	Deny	Permit	Deny	Permit	Permit	Permit	Permit	Permit	Permit																
Contractors	Deny	Deny	Custom	Deny	Deny	Custom	Custom	Permit	Permit	Custom																
Developers	Deny	Deny	Custom	Deny	Custom	Custom	Permit	Permit	Permit	Custom																
Development_S...	Deny	Deny	Deny	Deny	Deny	Custom	Permit	Permit	Deny	Permit																
Doctors	Permit	Permit	Permit	Permit	Permit	Custom	Permit	Deny	Permit	Permit																
Employees	Deny	Deny	Permit	Permit	Permit	Permit	Permit	Permit	Permit	Permit			Deny													Permit
Finance_Server...																										
Guests														Deny												
HVAC				Deny												Deny										

BYOD > **Default Policy** > HVAC
 HVAC > **Default Policy** > BYOD

BYOD → HVAC Default

Policy Status

Enabled ▼

Contract:

[Change Contract](#)

Policy Edit / Change Contract

BYOD -> HVAC

✕ [+ Create Contract](#)

🔼 Filter

Name ▲	Description	Policies Referencing
<input type="radio"/> Permit IP	Contract with access action as PERMIT	55
<input type="radio"/> Deny IP	Contract with access action as DENY	32
<input type="radio"/> Deny_TFTP_only	Access Contract for ISE SgAcls [Deny_TFTP_only]	0
<input type="radio"/> Allow_HTTPS_Deny_All		0
<input type="radio"/> PCI_Allowed_Traffic	DNAC Created SgacI	4
<input type="radio"/> BlockMalware		14

Show 10 entries

Showing 1 - 6 of 6

Previous **1** Next

Cancel

Change

Policy Edit / Change Contract



BYOD -> HVAC

+ Create Contract

🔍 Filter

Name ▲	Description	Policies Referencing
<input type="radio"/> Permit IP	Contract with access action as PERMIT	55
<input checked="" type="radio"/> Deny IP	Contract with access action as DENY	32
<input type="radio"/> Deny_TFTP_only	Access Contract for ISE SgAcls [Deny_TFTP_only]	0
<input type="radio"/> Allow_HTTPS_Deny_All		0
<input type="radio"/> PCI_Allowed_Traffic	DNAC Created SgacI	4
<input type="radio"/> BlockMalware		14

Show 10 entries

Showing 1 - 6 of 6

Previous 1 Next

Cancel

BYOD → HVAC ■ Deny

[View Policy Enforcement Stats](#) [View Traffic Flows](#)

Policy Status
Enabled ▼

Contract:
[Change Contract](#)

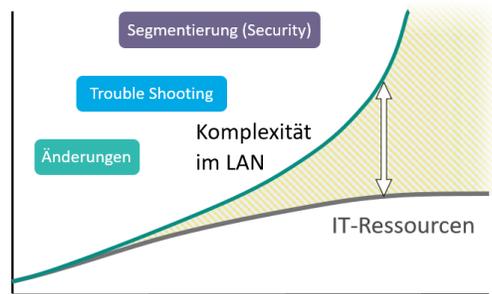
Name	Description	Policies Referencing
Deny IP	Contract with access action as DENY	33

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	DENY	advanced	TCP/UDP	Source Destination	104	OFF
2	DENY	advanced	TCP/UDP	Source Destination	1550	OFF
3	DENY	advanced	TCP/UDP	Source Destination	11112	OFF

Default Action DENY **Logging** OFF

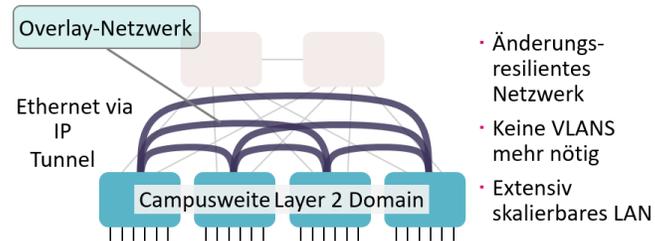
Zusammenfassung Teil 1

Warum SD-LAN



Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

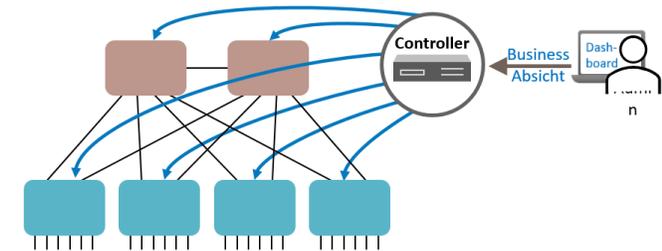
Logisches Overlay - Physisches Underlay



- Änderungs-resilientes Netzwerk (Change-resilient network)
- Keine VLANS mehr nötig (No VLANs needed)
- Extensiv skalierbares LAN (Extensively scalable LAN)

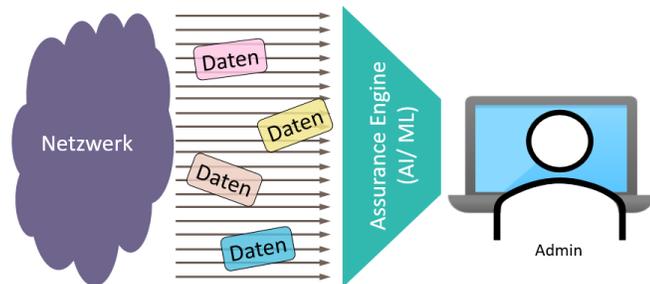
Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

...zum Intent Based Networking



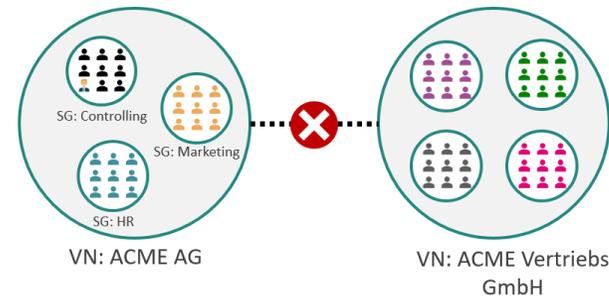
Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

Troubleshooting & Assurance



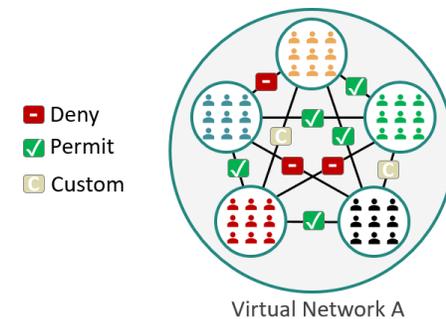
Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

Makro-Segmentierung → Zwischen Netzwerken



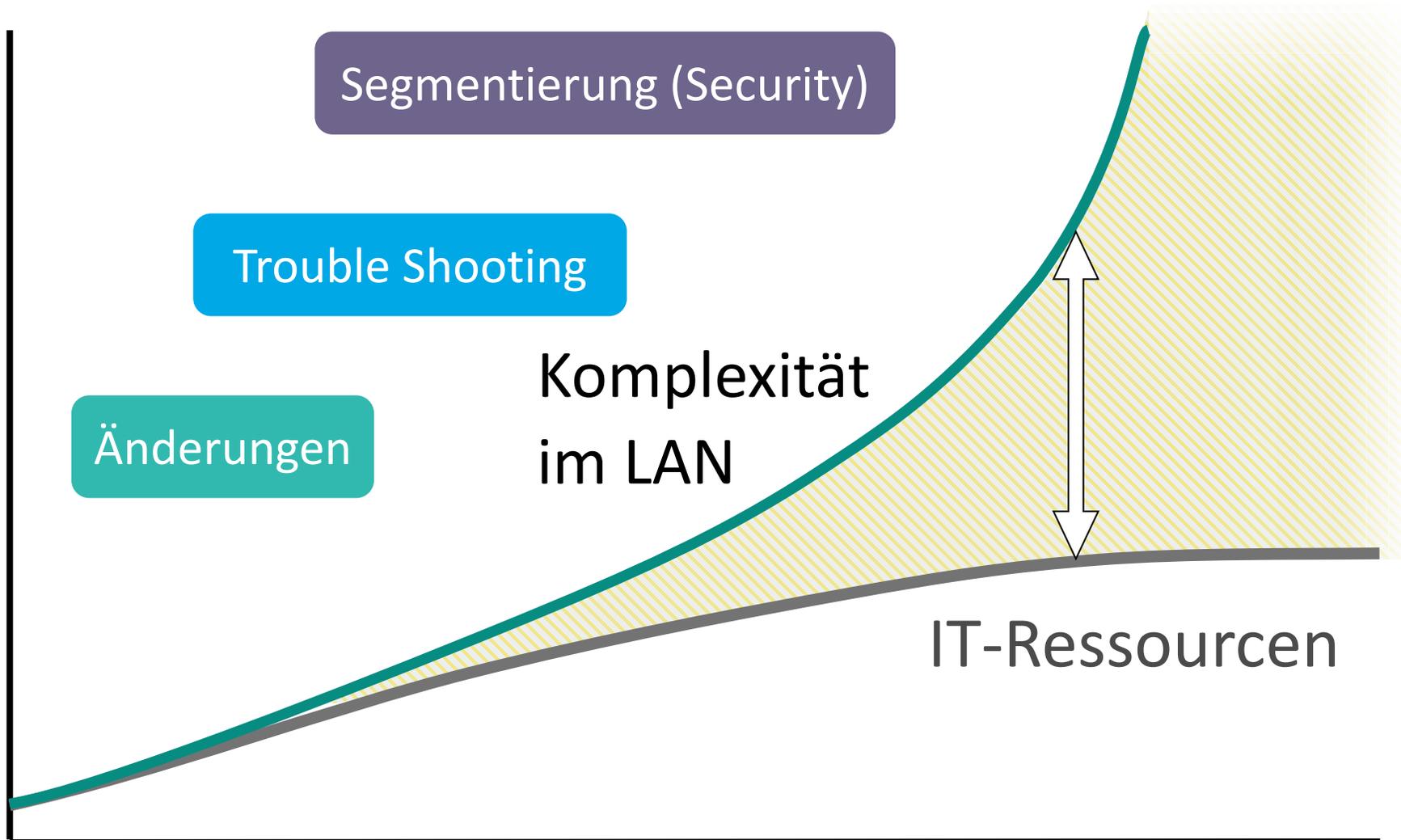
Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

Mikro-Segmentierung → Innerhalb eines Netzwerks

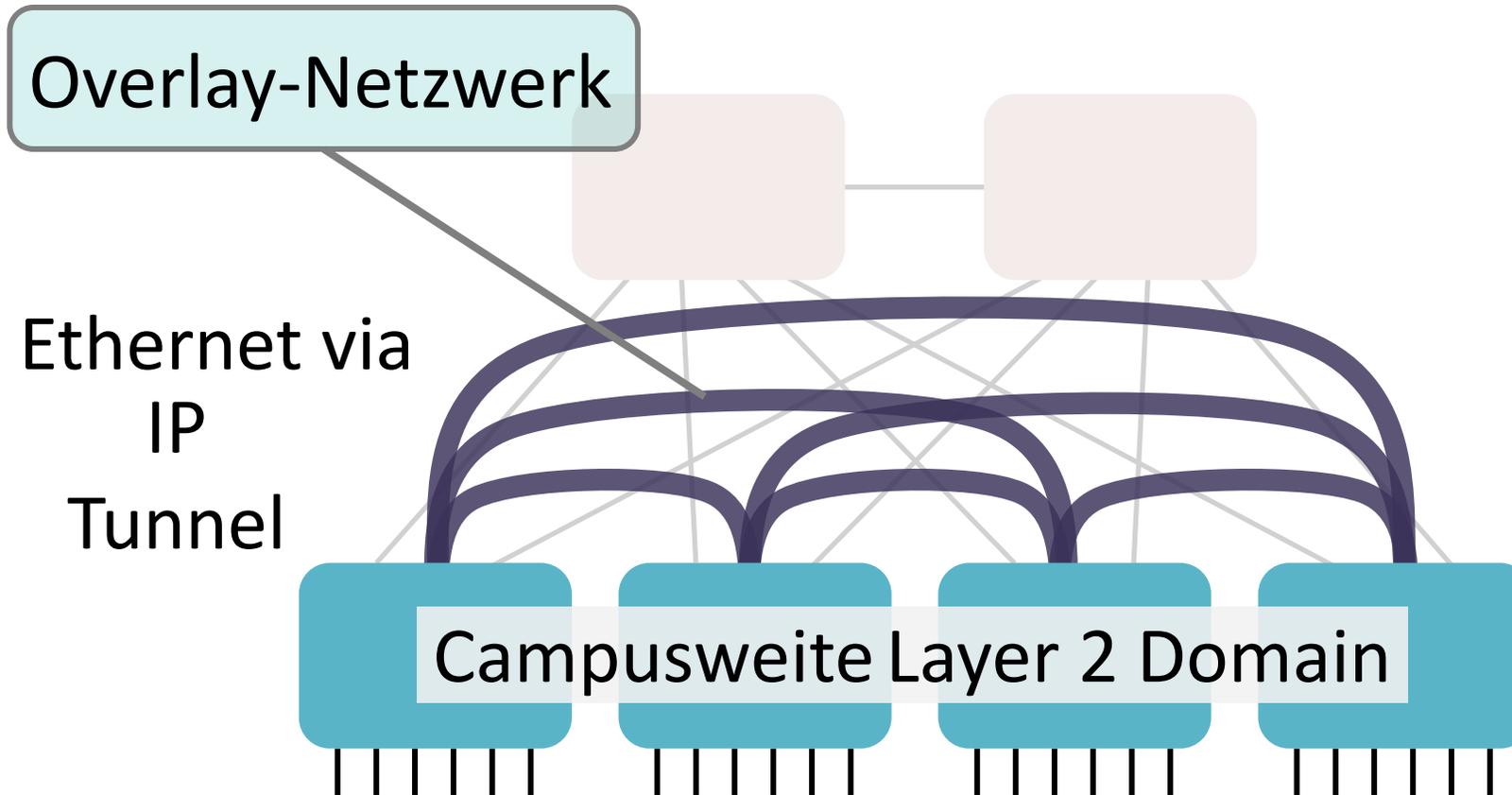


Next Generation LAN - SD-LAN - Nice to have oder lukrativer Business Case? - Frank Fäder

Warum SD-LAN

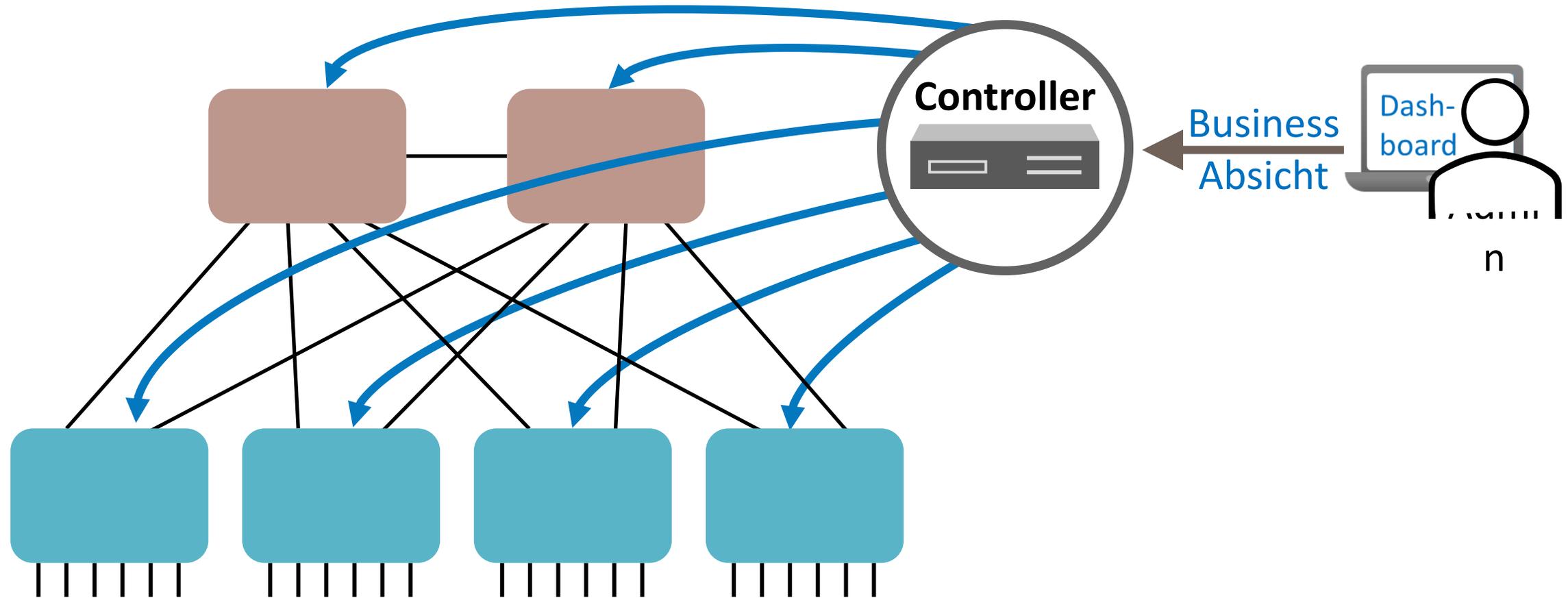


Logisches Overlay - Physisches Underlay

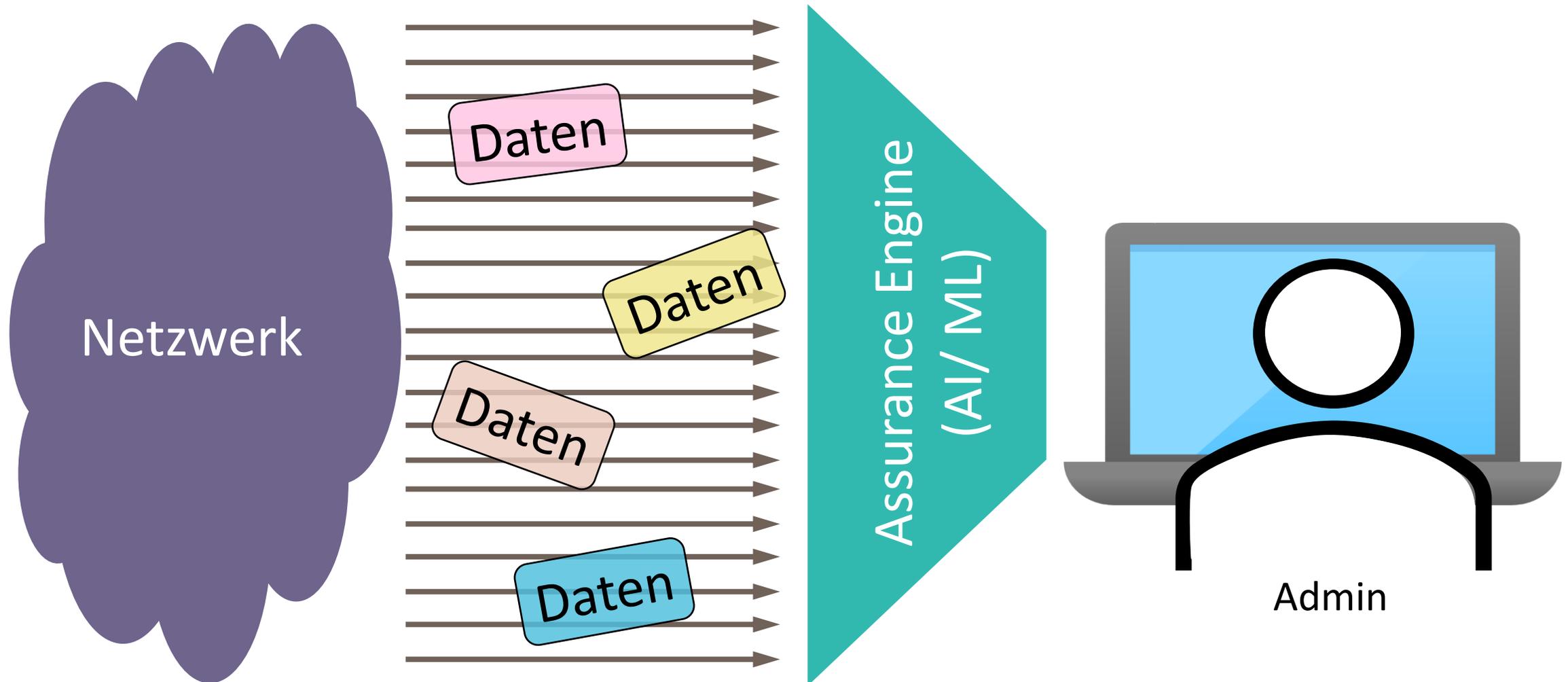


- Änderungs-resilientes Netzwerk
- Keine VLANs mehr nötig
- Extensiv skalierbares LAN

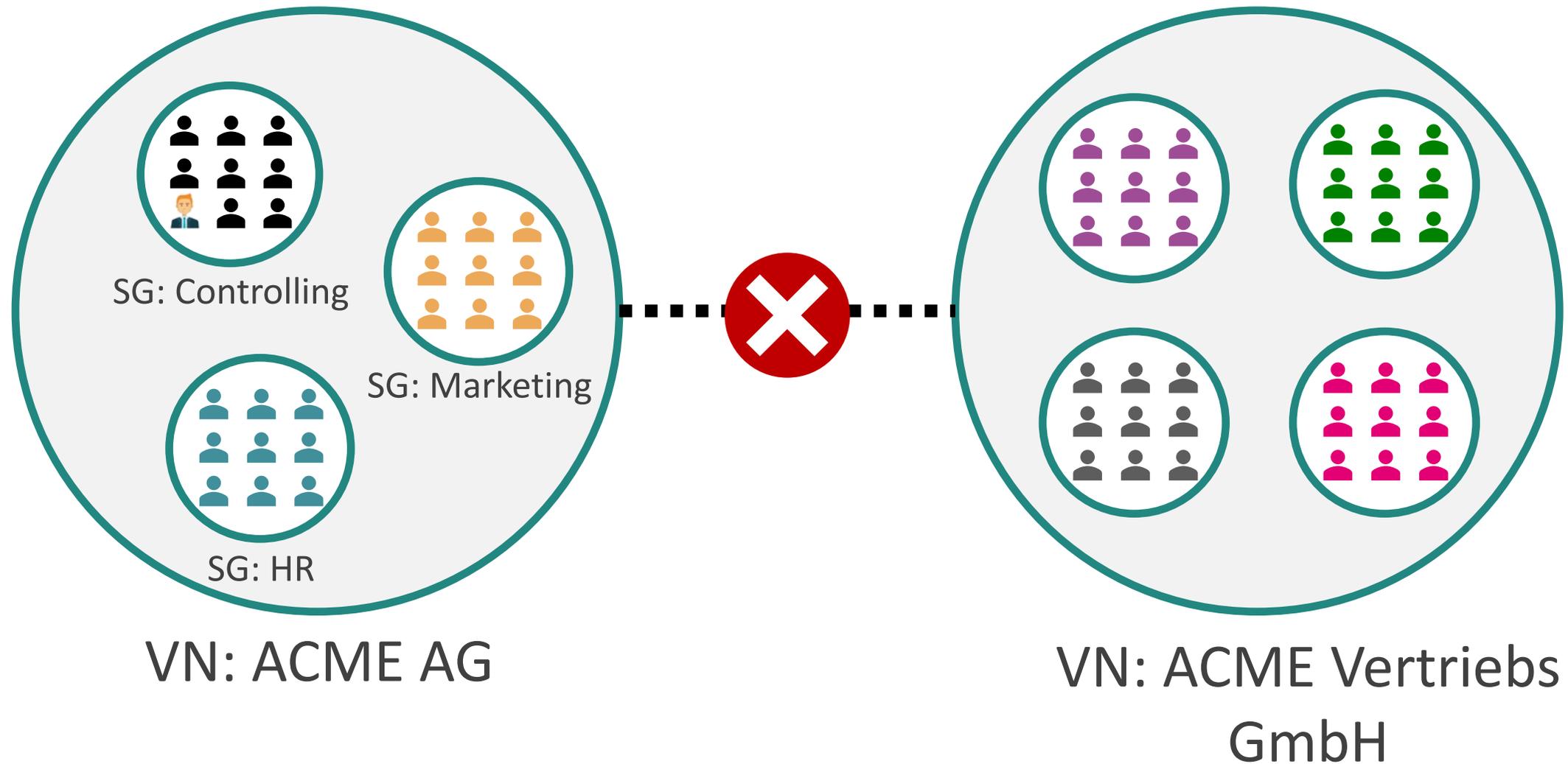
...zum Intent Based Networking



Troubleshooting & Assurance

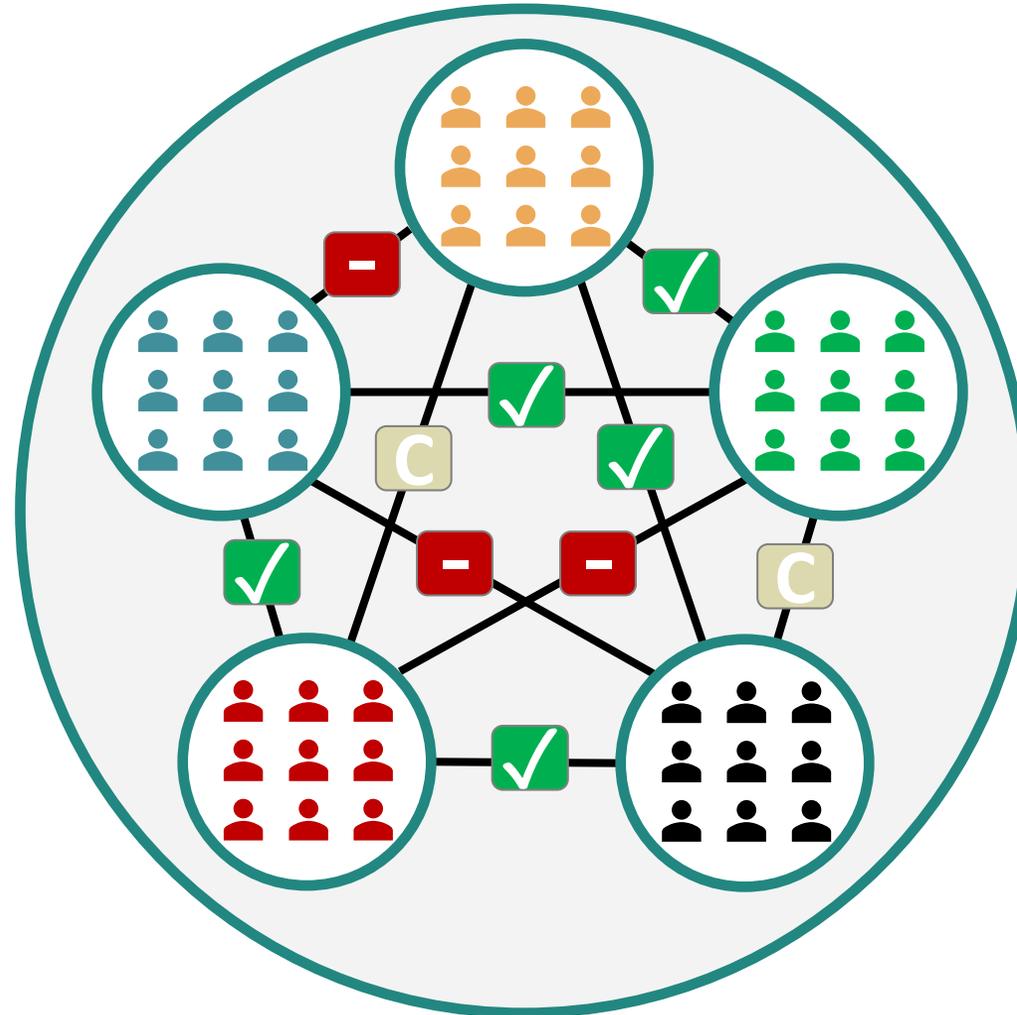


Makro-Segmentierung → Zwischen Netzwerken



Mikro-Segmentierung → Innerhalb eines Netzwerks

-  Deny
-  Permit
-  Custom



Virtual Network A



Kann man Security messen?

Gedanken zur Messbarkeit

1. Wenn es überhaupt eine Rolle spielt, ist es nachweisbar/ beobachtbar.
2. Wenn es beobachtbar ist, kann es als Menge (oder als Bereich möglicher Mengen) identifiziert werden.
3. Wenn es als Bereich möglicher Mengen identifiziert werden kann, kann es gemessen werden.

Hubbard, Douglas & Seiersen, Richard | How to Measure Anything in Cybersecurity Risk

Eine Messung ist eine quantitativ ausgedrückte
Verringerung der Unsicherheit
auf der Grundlage einer
oder mehrerer Beobachtungen.

Qualifizierte Schätzung:

Risiko eines „erfolgreichen Angriffs in den nächsten 36 Monaten

Berechnen

Nehmen Sie die Menge aller mit Ihnen vergleichbare Unternehmen bzgl. Cyber Risk an. Greifen Sie davon willkürlich 100 heraus.

Wie viele, schätzen Sie, erfuhren davon **in den letzten 12 Monaten** einen **erfolgreichen Angriff** durch einen der folgenden Vektoren:

1. Gestohlene/ kompromittierte Credentials
2. Phishing
3. Cloud Misskonfiguration
4. IoT Devices, Legacy Systems
5. Sonstige (z.B. Third Party Software, kompromit. Remotezugänge)

Qualifizierte Schätzung: Finanzielle Auswirkungen eines erfolgreichen Angriffs

Berechnen

In **95 von 100** Fällen eines erfolgreichen Angriffs beträgt der/ die/ das...

Betroffener Bereich	mehr als...	weniger als...
Ausfall des Kernprozesses in Tagen	7	21
Beeinträchtigung der Wertschöpfung in %	30%	95%
Aufwand Recovery/ Forensik in Tagen (extern)	15	60
Gezahlte Lösegeld in % vom Umsatz	0,05%	5%
Angriffsbedingter Marketingaufwand in % vom Umsatz	0,1%	2%
Verluste durch kompromittierte Geschäftsgeheimnisse in % vom Umsatz	0,5%	5%

Qualifizierte Schätzung: Finanzielle Auswirkungen eines erfolgreichen Angriffs

Berechnen

Mit den durch SD-LAN gegebenen Vereinfachung der Segmentierung beträgt in **95 von 100** Fällen eines erfolgreichen Angriffs der/ die/ das...

Betroffener Bereich	mehr als...		weniger als...	
Ausfall des Kernprozesses in Tagen	7	1	21	5
Beeinträchtigung der Wertschöpfung in %	30%	5	95%	20
Aufwand Recovery/ Forensik in Tagen (extern)	15	5	60	10
Gezahlte Lösegeld in % vom Umsatz	0,05%	0,05%	5%	5%
Angriffsbedingter Marketingaufwand in % vom Umsatz	0,1%	0,01%	2%	0,05%
Verluste durch kompromittierte Geschäftsgeheimnisse in % vom Umsatz	0,5%	0,1%	5%	0,3%

Erst wägen, dann wagen!

Helmuth von Moltke

VIELEN DANK!

ANSPRECHPARTNER IT-FACHVERTRIEB - INFRASTRUKTUR



A city skyline at sunset, with several skyscrapers illuminated against a colorful sky. The scene is viewed from an elevated position, showing a mix of modern and older buildings.

GEMEINSAM GESTALTEN WIR DIE **DIGITALE ZUKUNFT!**



ERLEBEN, WAS VERBINDET.

JANNIS SOBOLEWSKI

Technical Sales Consultant Infrastructure

DEUTSCHE TELEKOM GESCHÄFTSKUNDEN-VERTRIEB GMBH

Hahnstraße 43 d, 60528 Frankfurt a.M.

Telefon +49 69 20060 4186

Mobil +49 170 6367204

E-Mail J.Sobolewski@telekom.de

A city skyline at sunset, with several skyscrapers illuminated against a colorful sky. The scene is viewed from an elevated position, showing a mix of modern and older buildings.

GEMEINSAM GESTALTEN WIR DIE **DIGITALE ZUKUNFT!**



ERLEBEN, WAS VERBINDET.

MAURICE MATERNE

Technical Sales Consultant Infrastructure

DEUTSCHE TELEKOM GESCHÄFTSKUNDEN-VERTRIEB GMBH

Hahnstraße 43 d, 60528 Frankfurt a.M.

Telefon +49 69 20060 4217

Mobil +49 151 11770740

E-Mail Maurice.Materne@telekom.de