



Round Table: Cloud und Branch Connector

Laurent Soria

Security Engineer
soria@avantec.ch

Agenda Round Table

- Ziele des Round Tables
- Einführung Zero Trust & SASE
- Was ist ein Cloud & Branch Connector?
- Zero Touch Provisioning (Demo)
- Use-Cases aus der Praxis
- Vorteile von Zero Trust SD-WAN im Überblick
- Offene Fragerunde & Diskussion

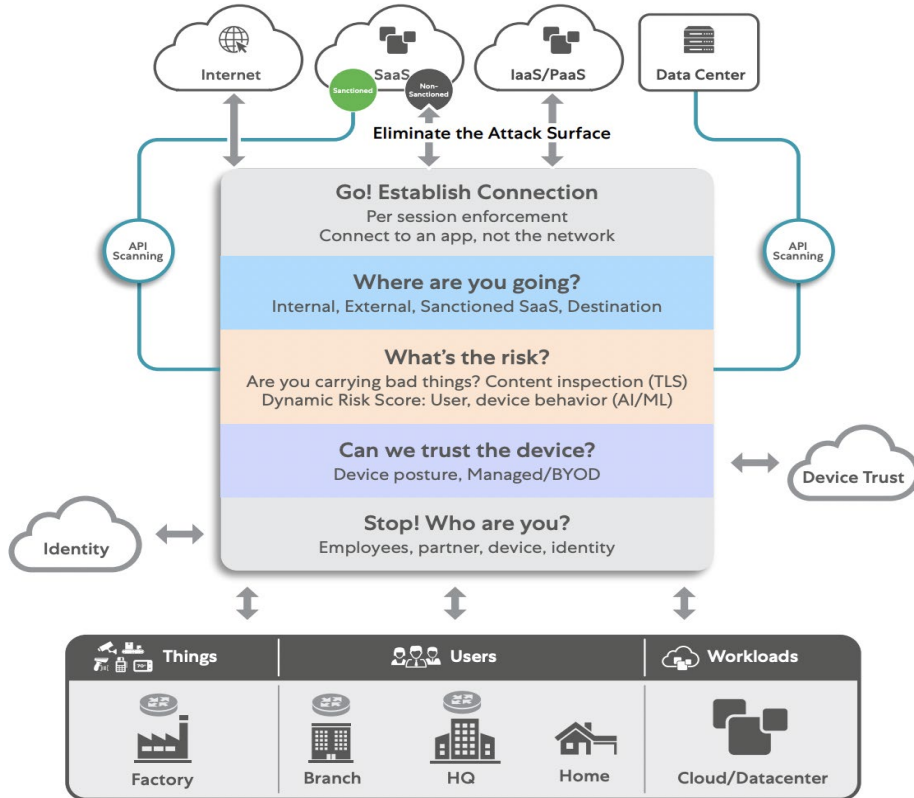
Ziele dieses Roundtables

- 1. Technische Funktionsweise und Mehrwert** der Cloud & Branch Connectoren nachvollziehen
- 2. Praxisbeispiele & Use-Cases** kennenlernen, um eigene Einsatzmöglichkeiten zu identifizieren
- 3. Möglichkeiten zur einfachen Integration in bestehende Infrastrukturen** erkennen
- 4. Erfahrungen** austauschen & **offene Fragen** klären



Einführung Zero Trust & SASE

Was ist Zero Trust?



3 Zero's

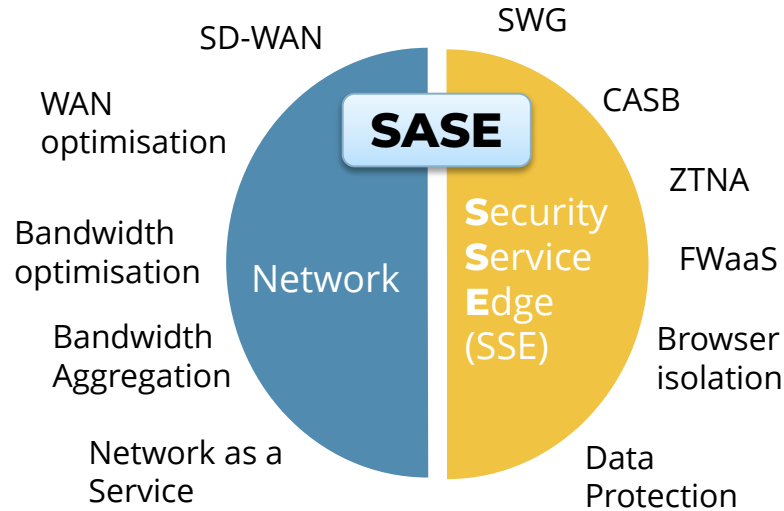
Connect
Zero network access

Inspect
Zero attack surface

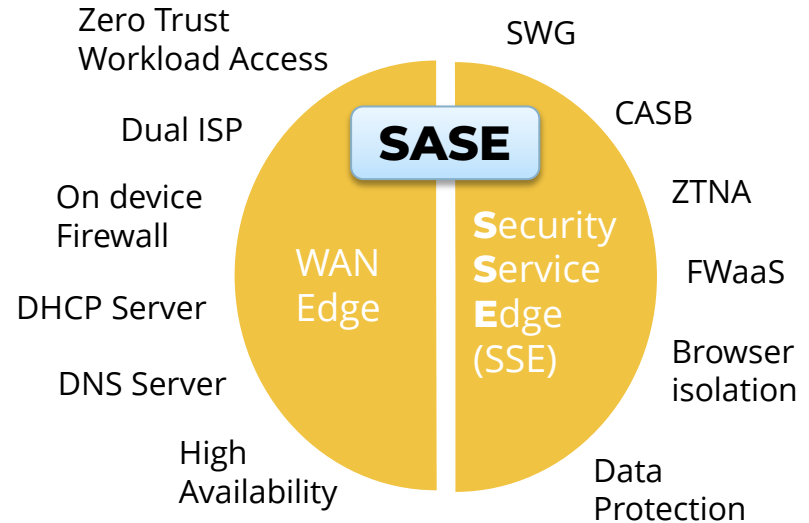
Verify
Zero Passthrough connections

SASE (Secure Access Service Edge)

SD-WAN + Zscaler SSE



Zscaler Zero Trust SD-WAN



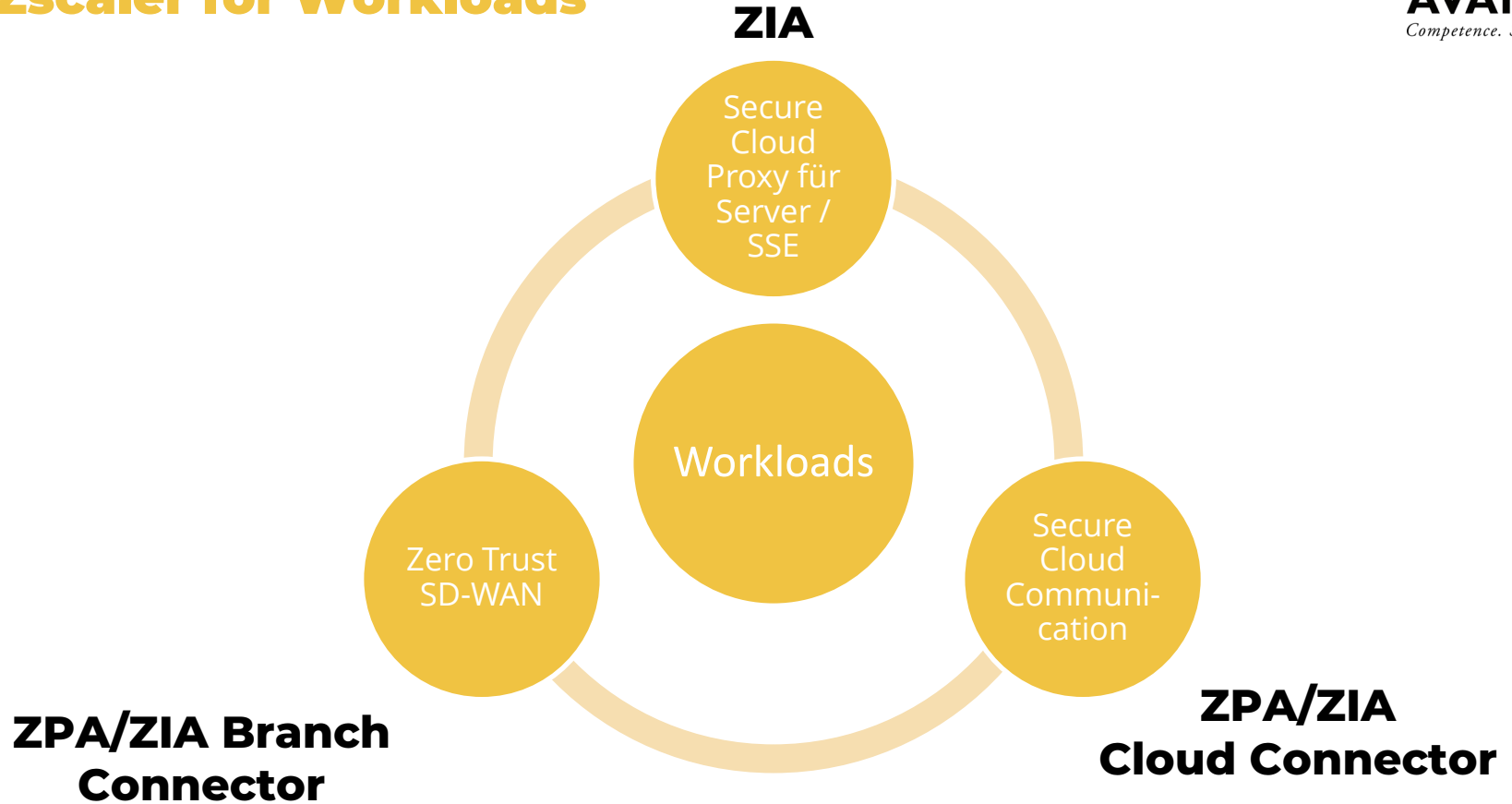
Was zählt zu «Workload» in der IT?

«Alles ausser User-Traffic»

Arbeitslast oder Ressource in der IT

- Physische Server
- Virtuelle Maschinen (Vmware, Hyper-V, etc.)
- Container (Docker, Kubernetes)
- Datenbanken & Webserver
- Serverless Functions (z.B. AWS Lambda)
- IoT / OT-Geräte & Industrieanlagen





Zscaler for Workloads

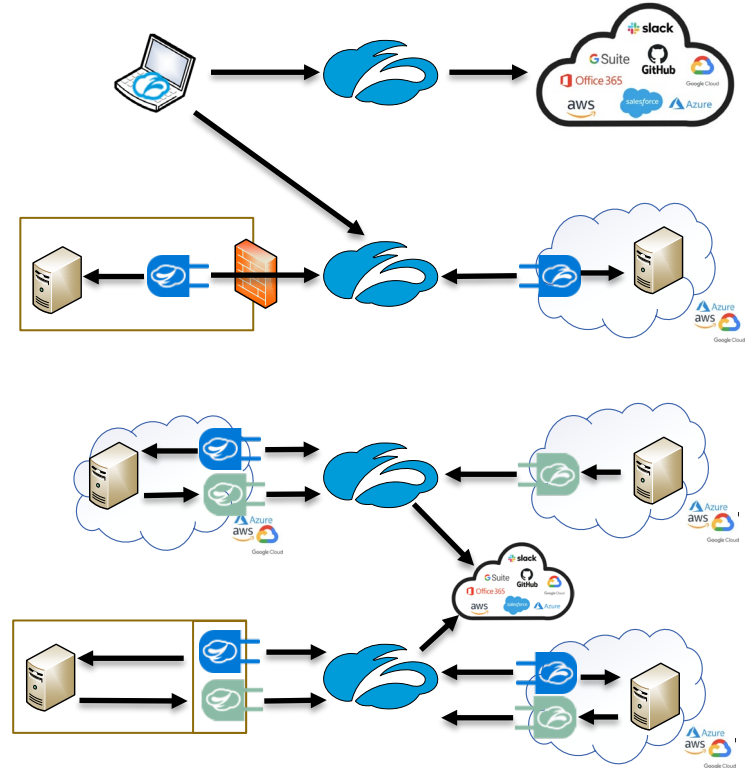




Was ist ein Cloud & Branch Connector?

Zscaler Connectoren

- **Zscaler Client Connector (ZCC)** 
 - ZIA: Verbindungen ins (public) Internet & SaaS
 - ZPA: Verbindungen zu (private) Workloads
- **App Connector** 
 - ZPA: «Proxy» zu Workloads
- **Cloud Connector** 
 - ZIA: Verbindungen ins (public) Internet & SaaS
 - ZPA: Verbindungen zu (private) Workloads
- **Branch Connector** 
 - Cloud + App Connector



Was ist ein Cloud & Branch Connector?



Cloud Connector

Einsatzbereich: IaaS- und PaaS-Umgebungen (Cloud)

Funktion: Sichere Verbindung von Cloud-Workloads zur Zscaler Zero Trust Exchange

Deployment: Als virtuelle Appliance verfügbar, skalierbar und zentral verwaltet



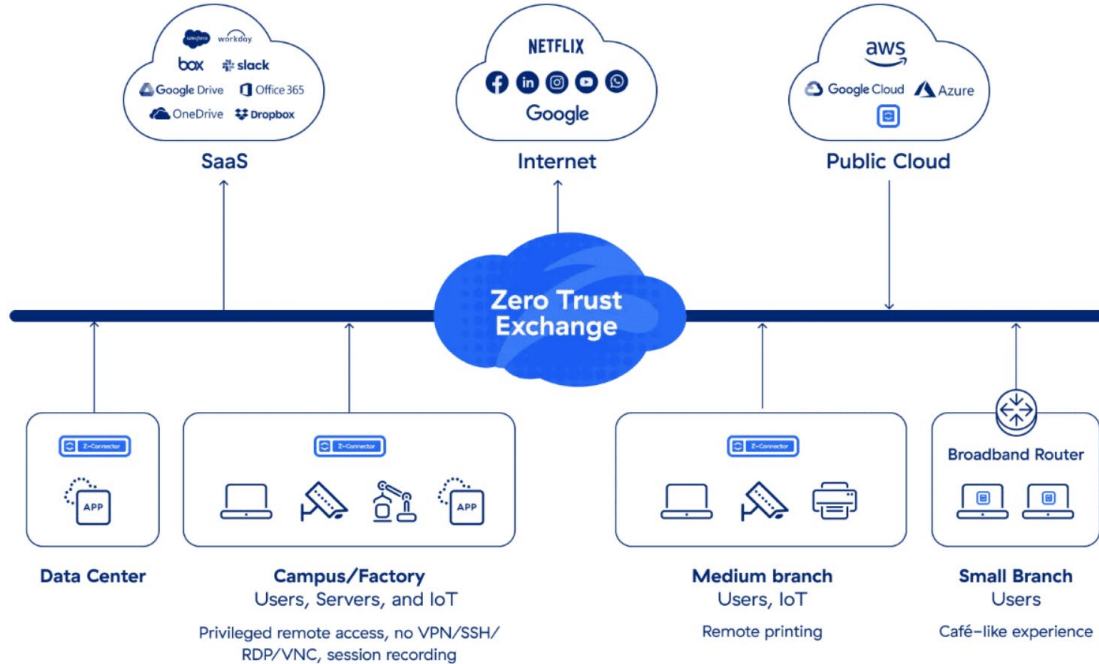
Branch Connector

Einsatzbereich: On-Premise in Branches, Datacenter, Produktionsstätten (IoT/OT), ...

Funktion: Anbindung an das ZTE, App Connector Integration möglich

Deployment: Physisch mit Zero Touch Provisioning oder VM

Cloud & Branch Connector



Cloud Connector

Lightweight VM

- Ressourcenschonend & schnelle Bereitstellung

Gehärtetes proprietäres OS

- Automatisierte Patches & Updates durch Zscaler

Hohe Verfügbarkeit (HA)

- Unterstützt native HA-Funktionalitäten von AWS und Azure

Skalierbare Performance

- Bis zu 500 Mbps pro Appliance



Google Cloud



Cloud-native Integration mittels Infrastructure-as-Code (IaC)

AWS CloudFormation



Terraform (GCP / Azure / AWS)



Marketplace (Azure / AWS)



Branch Connector

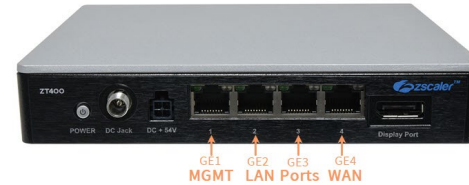
Hardware

- **ZT-400 (Small branches)**
200 Mbps, 4x GE-Interfaces
- **ZT-600 (Small / Medium branches)**
500 Mbps, 6x GE-Interfaces
- **ZT-800 (Medium / Large branches)**
1 Gbps, 6x GE-Interfaces + 2x SFP

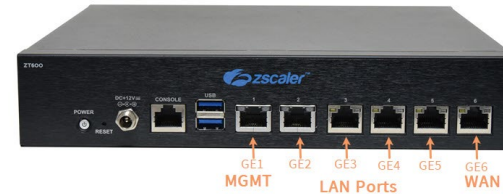
Virtuelle Maschine (VM)

- VMware ESXi (OVA) or Linux KVM
- Grosser Campus und Datencenter
- Multi-Gig Throughput

ZT400 (Gateway Mode)



ZT600 (Gateway Mode)



ZT800 (Gateway Mode)



Branch Connector mit 5G-Unterstützung

Zusätzliche Einsatzmöglichkeiten:

Standorte ohne kabelgebundenen Internetanschluss

- z.B. Event-Standorte, Baustellen, etc.

Redundanz & Ausfallsicherheit

- 5G als sekundärer Uplink bei ISP-Ausfall
- High Availability via Dual-WAN

Schnelle Inbetriebnahme

- Plug-and-Play-Deployment über 5G
- Keine Abhängigkeit von Netzwerkinfrastruktur



ZT 400-C

Branch Connector - Deployment Optionen

Non-Gateway / One-Arm Mode

Einsatzgebiete

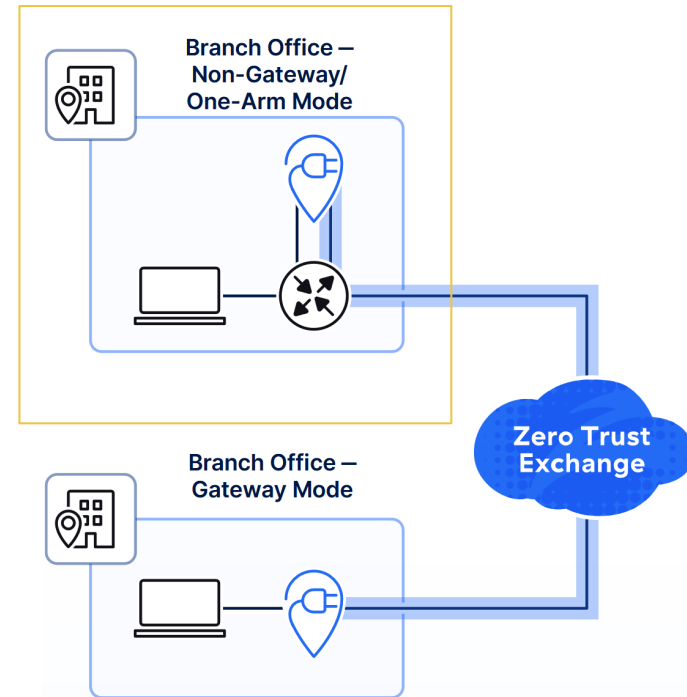
- z.B. Campus Area Network, Rechenzentren, M&A-Szenarien, IoT/OT-Anwendungen

Traffic-Steering

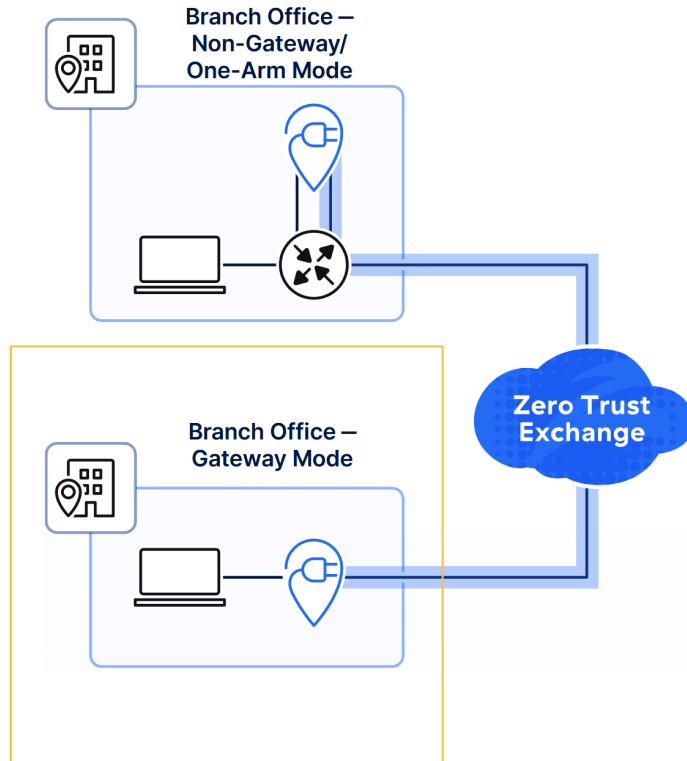
- Policy-Based Routing
- Conditional DNS Forwarding
(Minimale Änderung bestehendes Netzwerk)

Traffic Forwarding (Forwarder)

- Encapsulated in Tunnel zu ZTE
- Routing über bestehende Netzwerkgeräte



Branch Connector - Deployment Optionen



Gateway Mode (nur Hardware)

Einsatzgebiete

- z.B. Kleinere Standorte, Branches, Retail-Filialen mit wenig IT-Personal

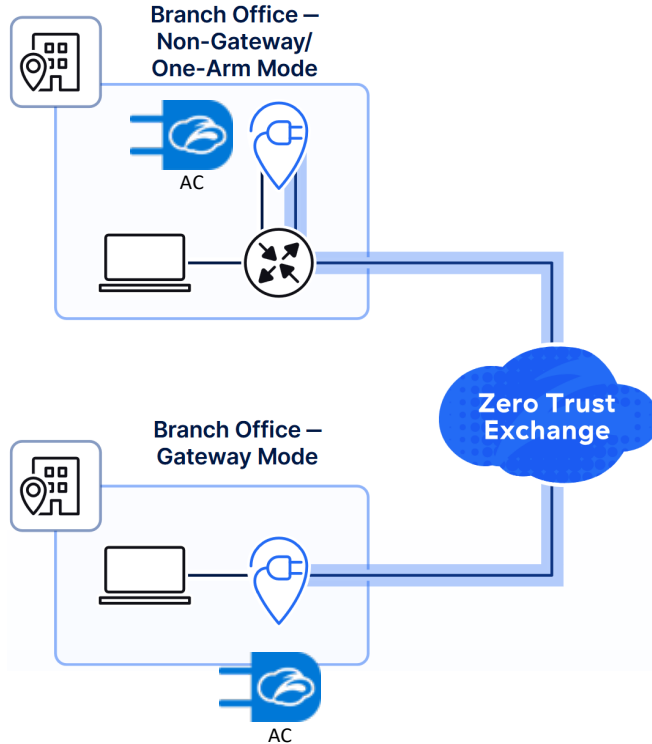
Traffic-Steering

- Branch Connector ist Default Gateway für das lokale Netzwerk

Zusatzfunktionen

- DHCP, VLAN Tagging
- High-Availability (HW und Dual ISP Support)

Branch Connector – App Connector



Built-in App Connector in Hardware & VM

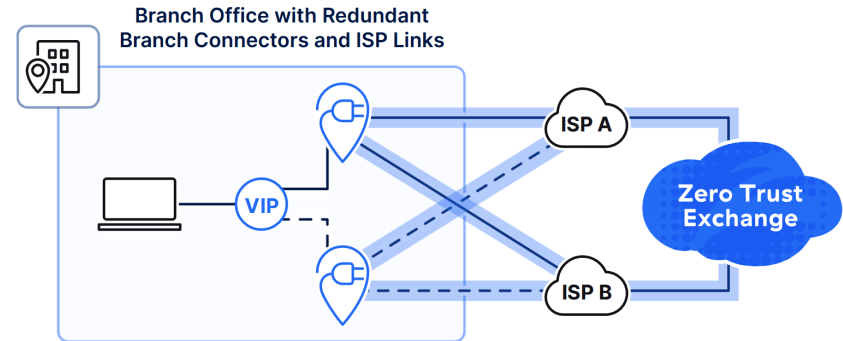
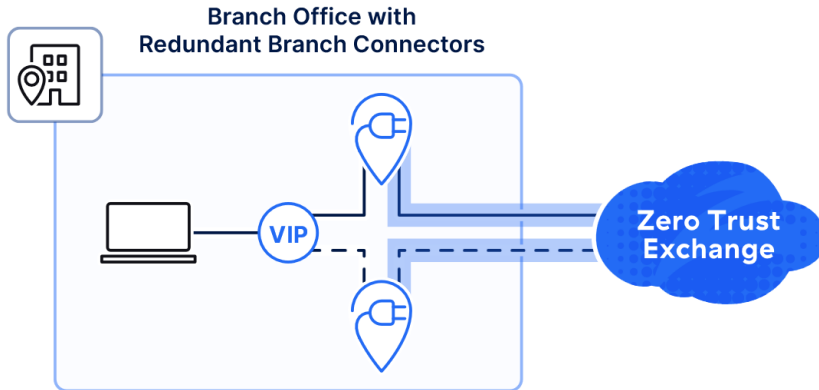
- Für beide Deployment Optionen möglich

Vorteile

- Zugriff auf Lokale Systeme / Applikationen
- Erkennung von Services durch App Discovery

(Nicht möglich bei Cloud Connector)

Branch Connector – High Availability



Branch Connector – Traffic Forwarding

Forwarding Rules

- Granulare Kontrolle für die Weiterleitung zu ZIA / ZPA
- Einrichten von Ausnahmen mit «direct»
- Verwerfen von ausgewählten Verbindungen mit «Drop»

Add Traffic Forwarding Rules

FORWARDING RULE

Rule Order: 5

Rule Name: FWD_5

Rule Status: Enabled

Forwarding Method: Direct

CRITERIA

General Services

Location/Sublocation: ---

Cloud & Branch Connector Groups

OR ---

Branch Connector – Traffic Forwarding GWs

ZIA Gateway [Log and Control Gateway](#) [DNS Gateway](#)

+ Add ZIA Gateway

Search

No.	Gateway Name	Primary Proxy	Secondary Proxy	Description	Fail Close
1	CH-gw	zrh1.svpn.zscaler.net	Auto		not-active
2	DE-gw	muc1.svpn.zscaler.net	fra6.svpn.zscaler.net	To use Germany	not-active
3	Default ZIA Gateway	Auto	Auto	Automatically created zia gateway	active
4	UK-gw	lon3.svpn.zscaler.net	lon5.svpn.zscaler.net	Use LON gateway	not-active

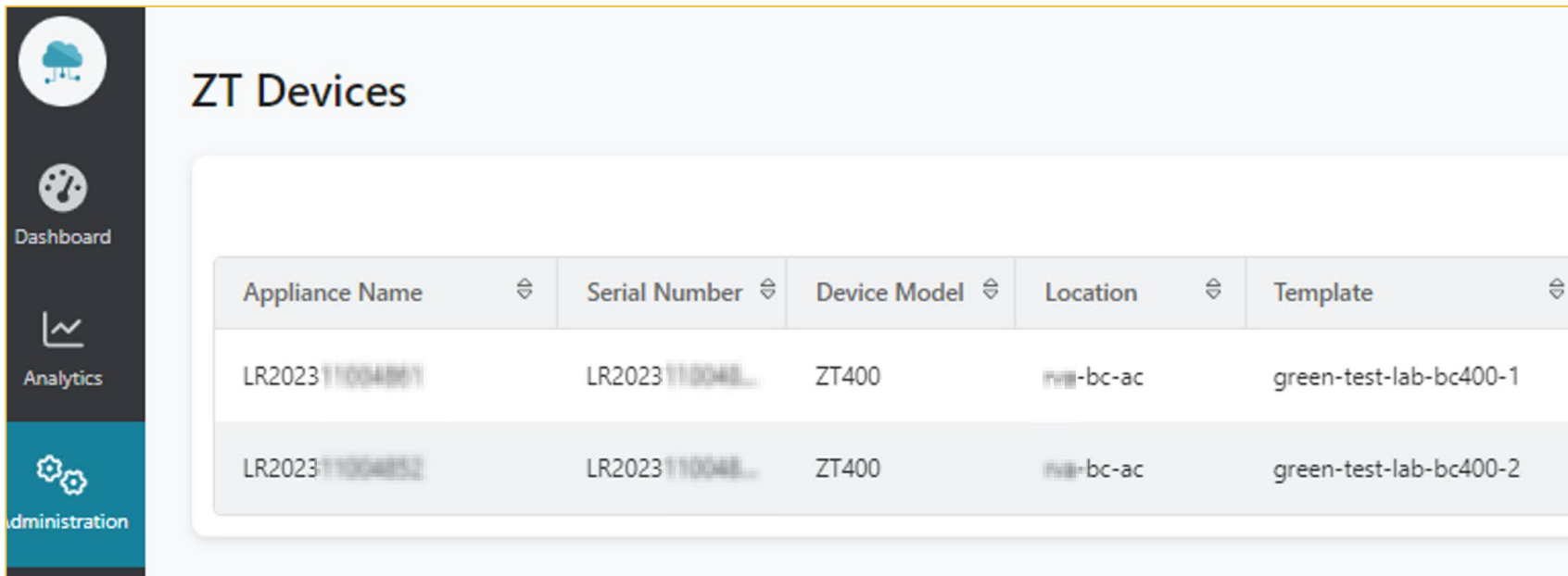
Branch Connector – Traffic Forwarding Beispiel

Rule Name	Criteria	Forwarding Method	Status	Description
FWD_AppleTV_Netflix	<p>DESTINATION ADDRESSES *.netflix.com</p> <p>LOCATIONS home</p> <p>SOURCE IP ADDRESSES 192.168.1.100</p>	ZIA	Enabled	DESCRIPTION Forward to DE / CH



Zero Touch Provisioning (Demo)

Zero Touch Provisioning – Gateway Mode



Appliance Name	Serial Number	Device Model	Location	Template
LR202311004801	LR2023110048...	ZT400	lab-bc-ac	green-test-lab-bc400-1
LR202311004802	LR2023110048...	ZT400	lab-bc-ac	green-test-lab-bc400-2

Zero Touch Provisioning – Gateway Mode

Edit Branch Connector Provisioning Template




- General Information
- Location
- Branch Connector Group
- Device Details
- App Connector
- Review

General Information


Configure a Branch Connector Provisioning Template within the Zscaler Cloud & Branch Connector Admin Portal to deploy Branch Connector as a virtual machine in your branch account or data center. For more information, view the [Getting Started](#) document.

Name
green-test-lab-GW-zbc400-1

Hypervisor

Hardware Device



Deploy as Gateway

Yes No

Cloud Provider

✓ General Information

○ Cloud Provider

● Location

● Group Information

● Review

Cloud Provider

Select one of the following cloud providers.

Cloud Provider



Zero Touch Provisioning – Gateway Mode

- General Information
- Location**
- Branch Connector Group
- Device Details
- App Connector
- Review

Location

Select a location for your Branch Connector Provisioning Template.

Location Type

Existing

Location Name

AVA-Zurich

Country

Switzerland

Location Template

TEST-BRC

- General Information
- Location
- Branch Connector Group**
- Device Details
- App Connector
- Review

Branch Connector Group

Fill out the information below for your Branch Connector Group.

Branch Connector Group Type

Existing

Branch Connector Device Group

green-test-lab-GW-bc400-group

Description (Optional)

Auto created from 991a2204-76f6-49e3-a762-bdaf08dfcce3

BC in gateway mode

Location Templates

The screenshot shows the 'Location Templates' management page. On the left is a dark sidebar with navigation icons for Dashboard, Analytics, and Administration. The main content area has a header with 'Location Templates' and 'Locations'. Below the header is a blue button labeled '+ Add Location Template'. At the bottom, there is a table with one entry.

No.	Name
1	Default Location Template

The screenshot shows the 'Add Location Template' configuration dialog. It has a blue title bar with a close button. The dialog contains two input fields: 'Name' with the value 'Zürich' and 'Template Prefix' with the value 'ZRH'. Below these is a section titled 'GATEWAY OPTIONS' containing five toggle switches, all of which are currently turned off.

Add Location Template

Name: Zürich Template Prefix: ZRH

GATEWAY OPTIONS

- Enable XFF Forwarding:
- Enforce Authentication:
- Enable Caution:
- Enable AUP:
- Enforce Firewall Control:

Zero Touch Provisioning – Gateway Mode

- General Information
- Location
- Branch Connector Group
- Device Details**
- App Connector
- Review

System Settings

Device Model	Device Serial No	LR2023
ZT400	Device Name	LR2023
	Description (Optional)	Device green-test-lab-bc400-1 in AVA-LAB

Management	Shutdown	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Interface	DHCP	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
(GE1)	IP Address	<input type="text"/>	
	Default Gateway IP Address	<input type="text"/>	
	Primary DNS	<input type="text"/>	
	Secondary DNS	<input type="text"/>	

Zero Touch Provisioning – Gateway Mode

- General Information
- Location
- Branch Connector Group
- Device Details**
- App Connector
- Review

WAN

WAN needs a minimum of one interface or sub-interface enabled, and a maximum of two interfaces or sub-interfaces enabled.

[+Add Interface](#)

GE4

Interface	Name	GE4
	MTU	1500

IP Info

Description (Optional) WAN

DHCP Enabled Disabled

IP Address

Default Gateway IP Address

Primary DNS Server

Secondary DNS Server

Uplink Mode Active Standby

[+Add IP Info](#)

[+Add Sub Interface](#)

Zero Touch Provisioning – Gateway Mode

- General Information
- Location
- Branch Connector Group
- Device Details**
- App Connector
- Review

LAN

LAN needs a minimum of one interface or sub-interface enabled.

GE2 [+Add Interface](#)

Interface	Name
	GE2

Shutdown Yes No

MTU 1500

IP Info

Description (Optional) LAN

IP Address 192.168.1.3/24

High Availability Enabled Disabled

DHCP Server Enabled Disabled [×](#)

[+Add IP Info](#)

[+Add Sub Interface](#)

DNS Server

Use WAN DNS Server Yes No

Routing

Static Route (Optional)

Route	Gateway
XXXXXX	XXXX

[+Add More](#)

Zero Touch Provisioning – Gateway Mode

- ✓ General Information
- ✓ Location
- ✓ Branch Connector Group
- ✓ Device Details
- App Connector
- Review

App Connector

App Connectors can be provisioned as part of this template. Please fill in the information below or skip to the next step.

App Connector

Enabled Disabled

Zero Touch Provisioning – Gateway Mode

- General Information
- Location
- Branch Connector Group
- Device Details
- App Connector**
- Review

App Connector

App Connectors can be provisioned as part of this template. Please fill in the information below or skip to the next step.

App Connector

Enabled Disabled

Port 1 MGMT
Port 2 FWD & SRV
Port 3 AppC

Port 1 MGMT
Port 2 FWD & SRV
Port 3 AppC





App Connector Group Name ⓘ
AVA-LAB-TEST

App Connector Deployment Status
Active-Active

Zero Touch Provisioning – Gateway Mode



Name	OS	Status	Actions
BranchGruen	RedHat Linux	---	Ready to Deploy
green-test-lab-bc400-1	RedHat Linux	---	Deployed
green-test-lab-bc400-2	RedHat Linux	---	Ready to Deploy
bc-only	RedHat Linux	---	Ready to Deploy
green-test-lab-bc400-1	ZT400	LR2023 [redacted]	<input checked="" type="checkbox"/> Deployed
green-test-lab-bc400-2	ZT400	LR2023 [redacted]	<input type="checkbox"/> Staged <input checked="" type="checkbox"/> Ready to Deploy

Zero Touch Provisioning – Gateway Mode



Dashboard

Analytics

Administration

Branch Devices

Physical Virtual

<input type="checkbox"/> Name	Branch Type	Serial Number	Location	Upgrade Window 	Operational Status	HA Status	Upgrade Status
<input type="checkbox"/> ▼ green-test-lab-bc400-group			bc-ac	Thursday 1:00 AM - 3:00 AM Europe/Zurich	● 1	---	🕒 Scheduled
<input type="checkbox"/> green-test-lab-bc400-group-VM-lkQtM	ZT400	LR20231 	bc-ac	Thursday 1:00 AM - 3:00 AM Europe/Zurich	● Active	● Active	🕒 Scheduled

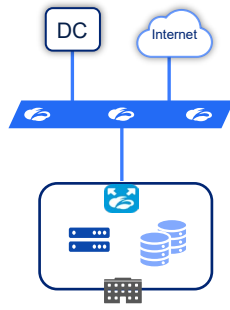


Use-Cases aus der Praxis

Key Use Cases

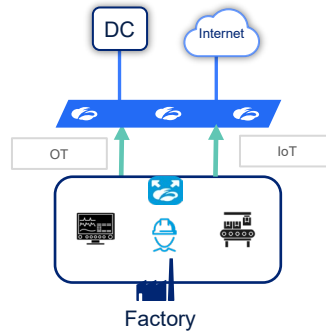
S2S VPN Ersatz

Zero Trust for Server



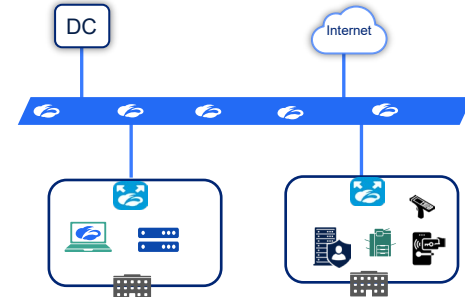
Optimierung von IoT/OT Anbindung

Zero Trust for IoT/OT

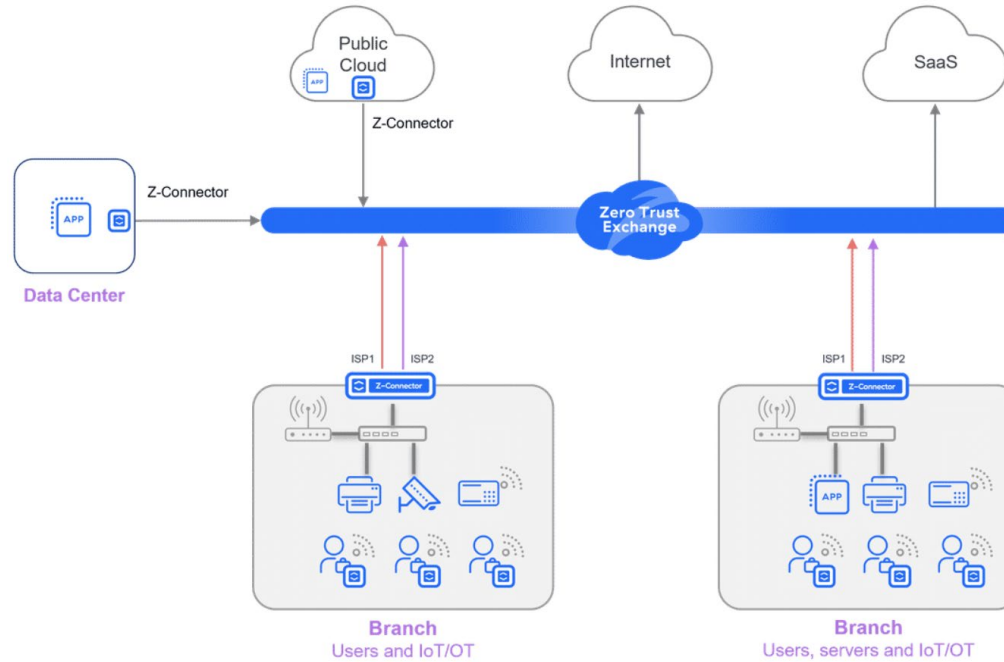


M&A IT Integration

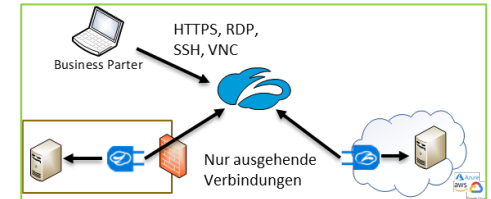
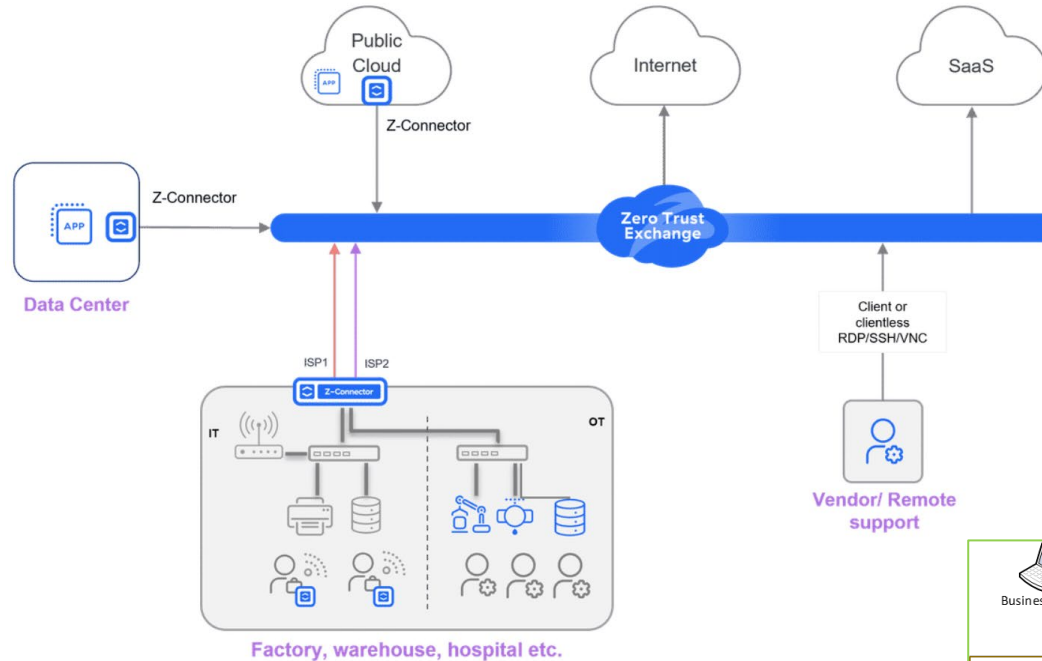
Zero Trust Site-to-Site



Use Case – S2S VPN Ersatz



Use Case – Optimierung von IoT/OT Anbindung

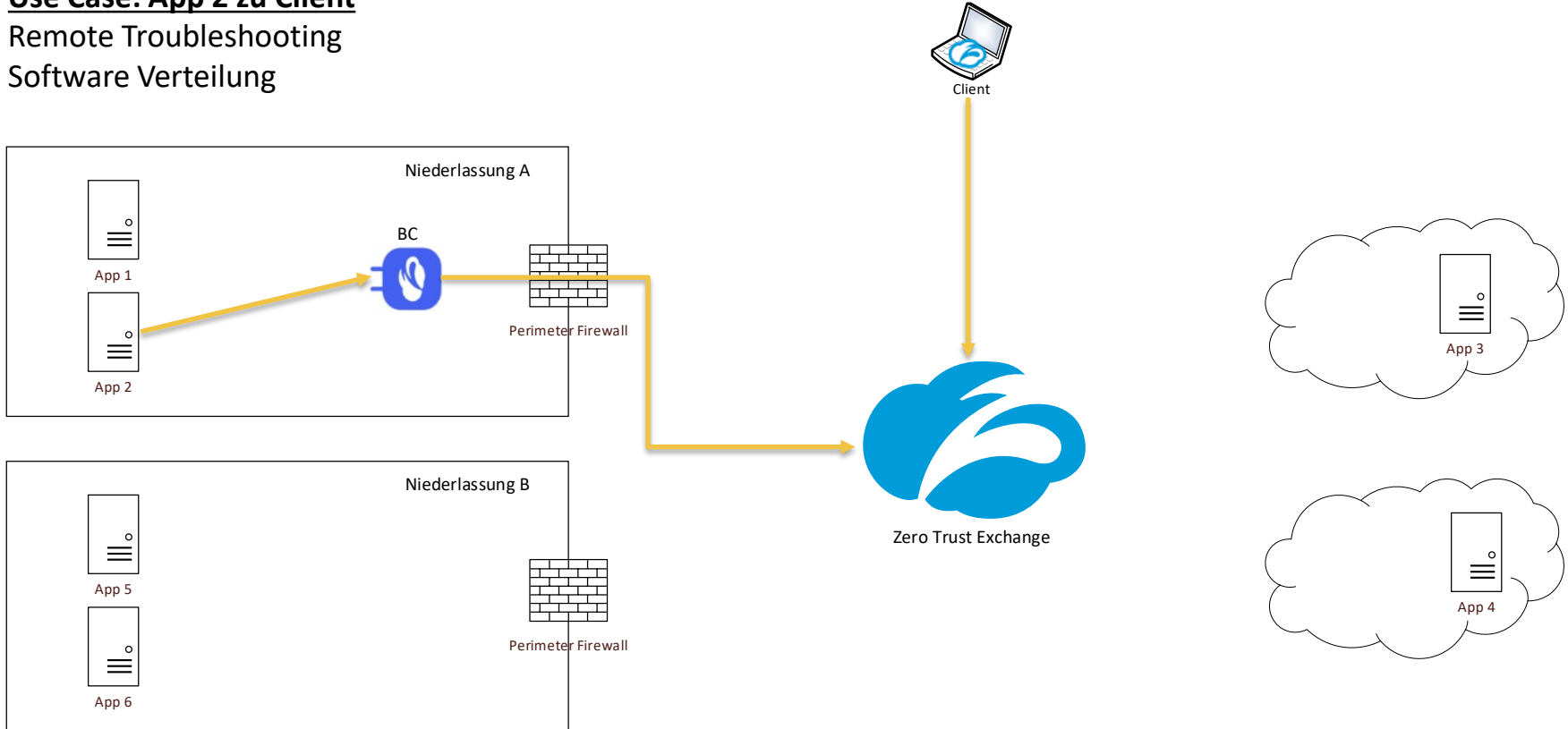


Use-Case – Server zu Client Verbindung

Use Case: App 2 zu Client

Remote Troubleshooting

Software Verteilung

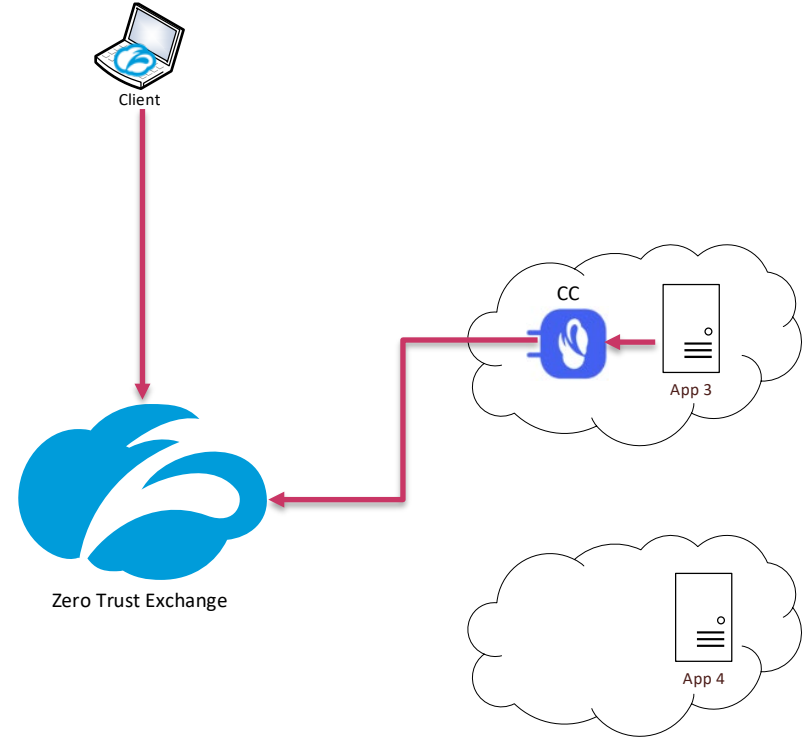
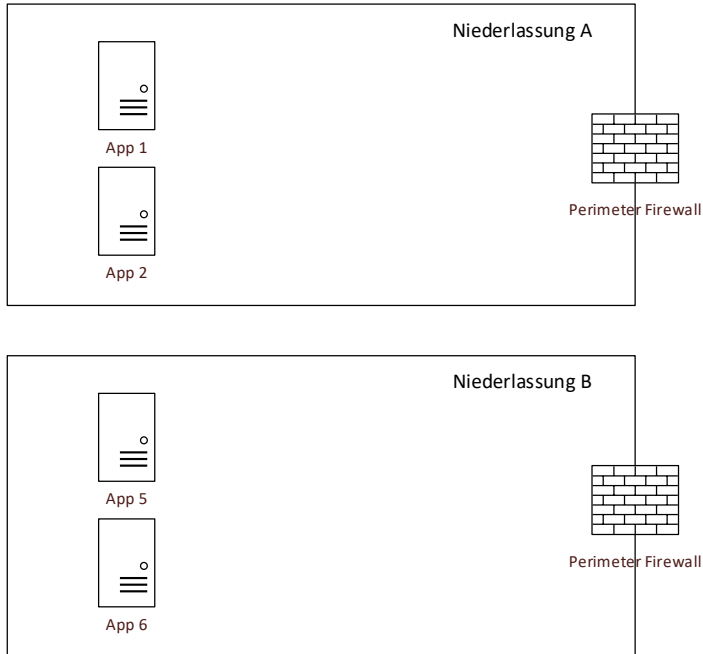


Use-Case - Server zu Client Verbindung

Use Case: App 3 zu Client

Remote Troubleshooting

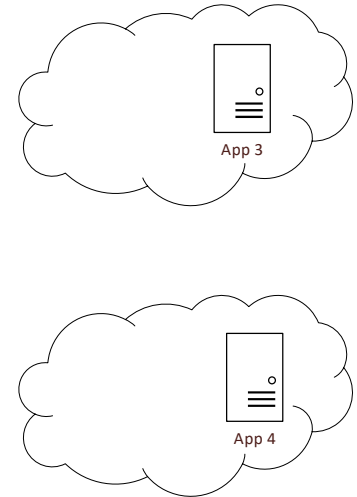
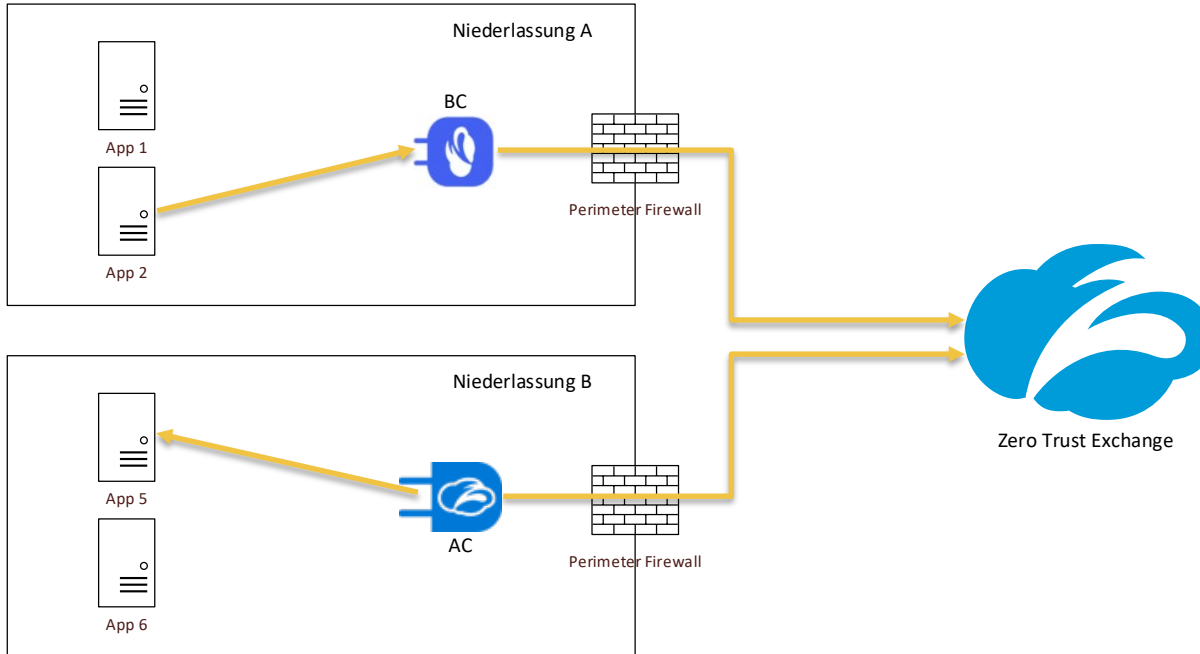
Software Verteilung



Use-Case - Workload zu Workload

Use Case: App 2 zu App 5

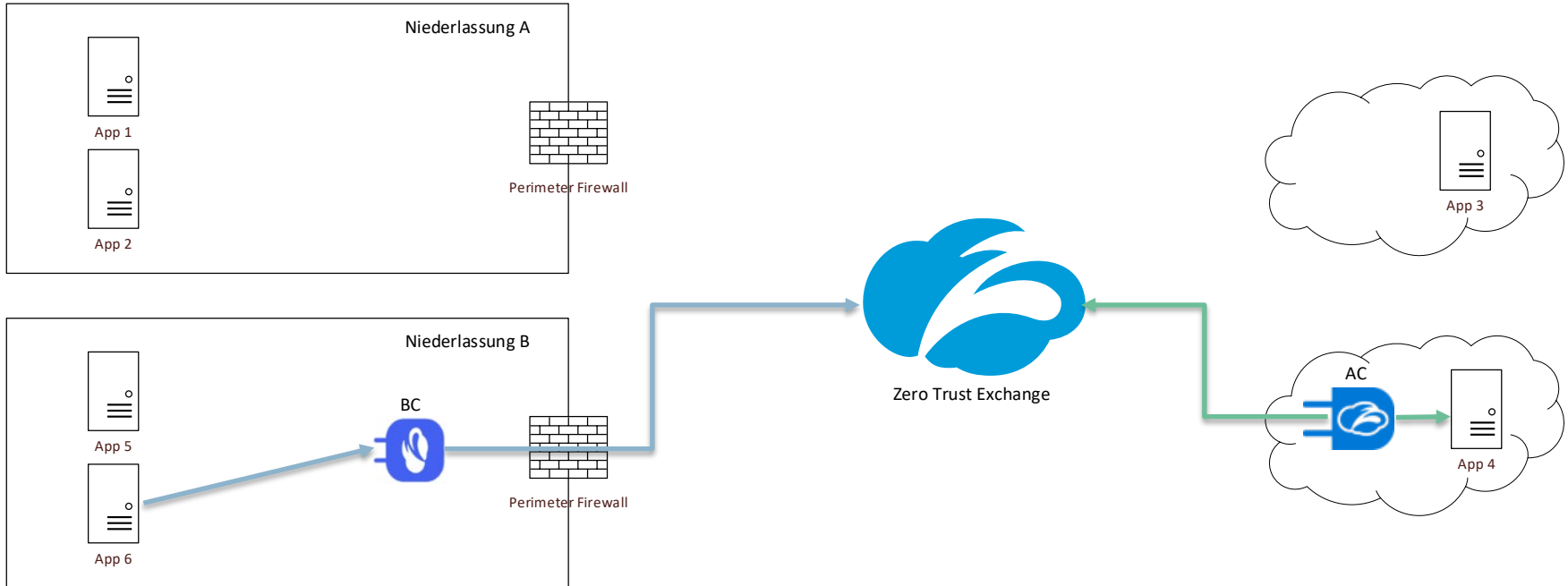
Site to Site VPN oder SD-WAN Ersatz



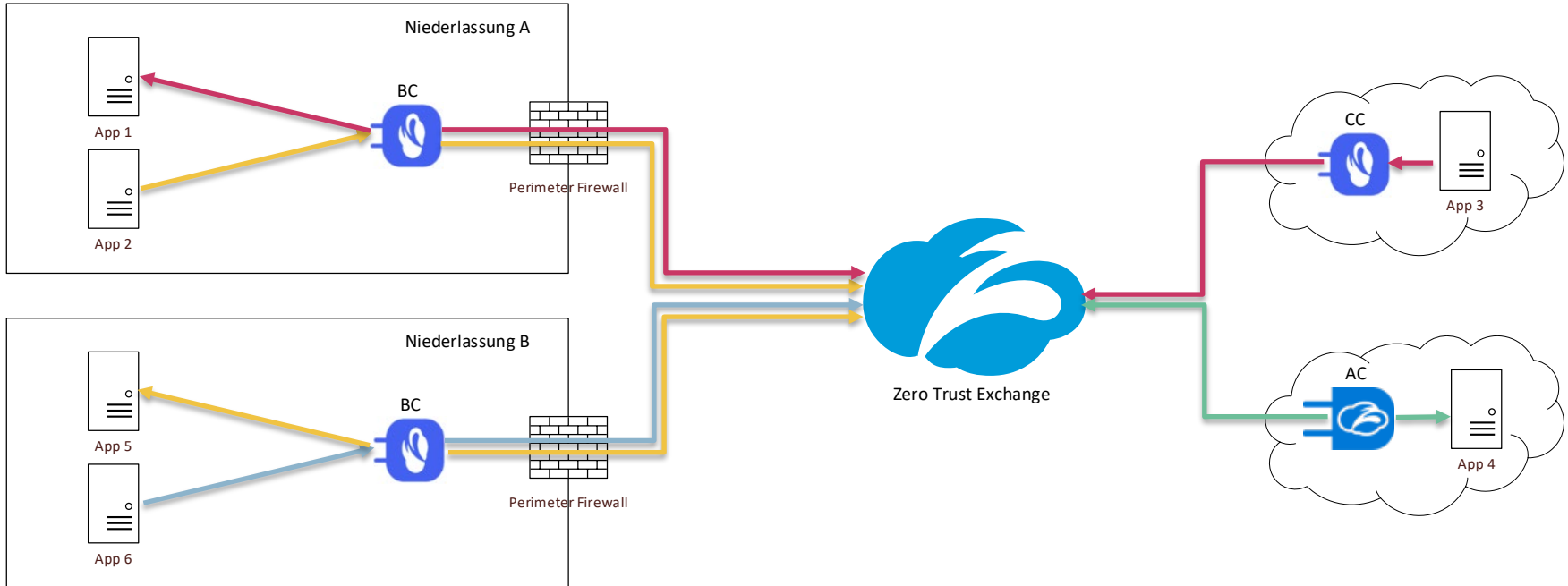
Use-Case - Workload zu Workload

Use Case: App 6 zu App 4

Site to Site VPN oder SD-WAN Ersatz



Use-Case - Server zu Server



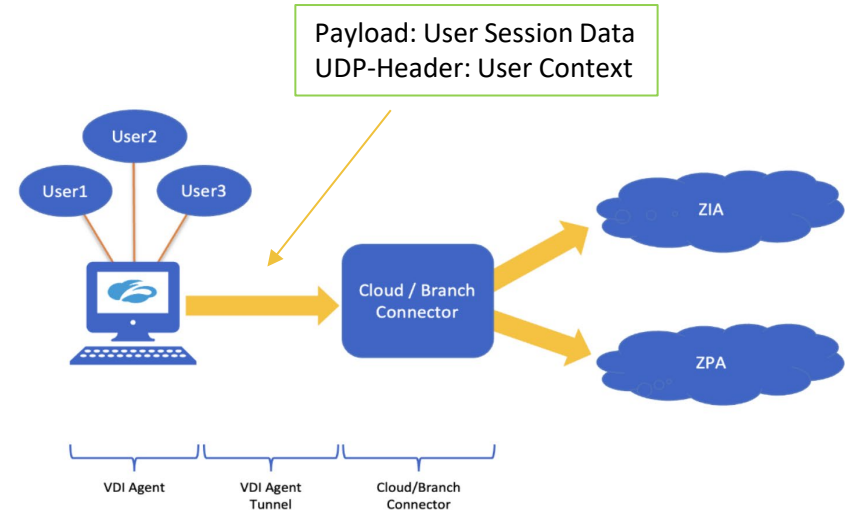
Use-Case – Umgebung mit Zscaler VDI Light Agent

Einsatzszenarien

- Multisession non-persistent VDI
 - User Zuweisung über Pool
- On-Premise oder in der Public Cloud

Funktionsweise des VDI Light Agent

- VDI Agent wird auf Master-Image installiert
- Alle User-Sessions teilen denselben Tunnel
- Tunnel geht über CC / BC
- Breakout über ZIA oder ZPA

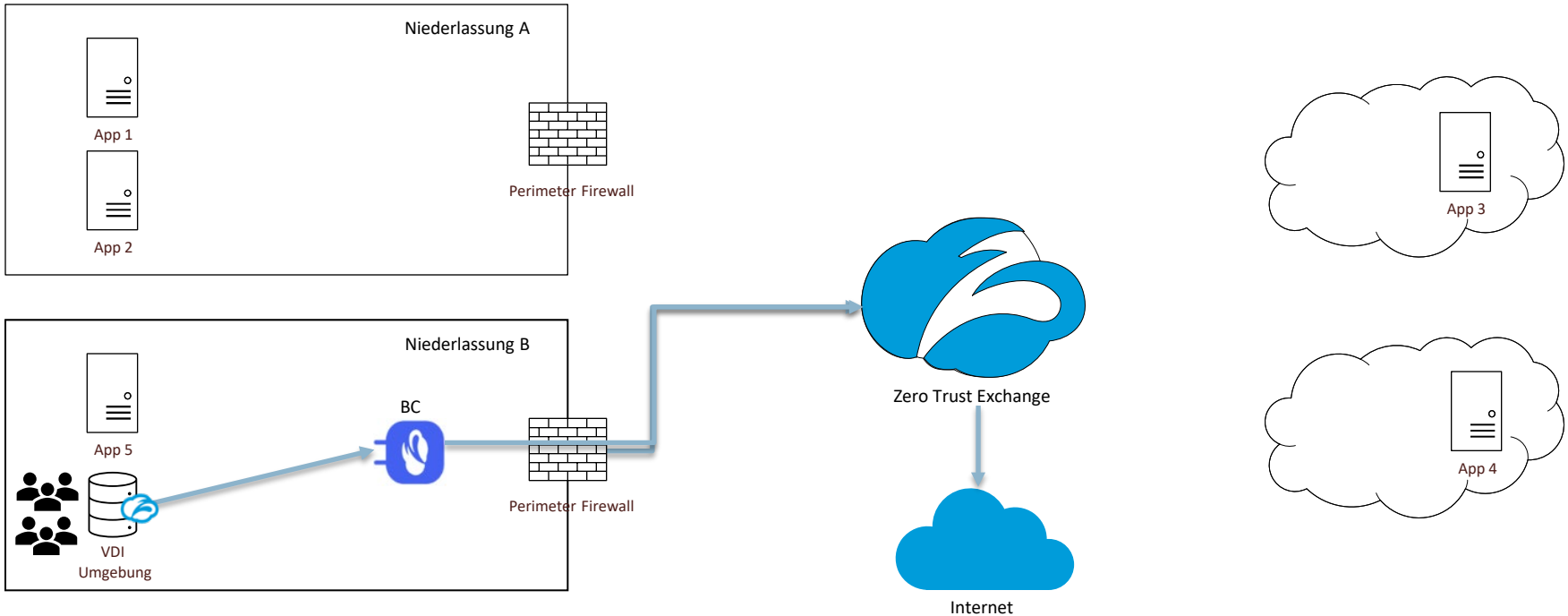


Use-Case - VDI zu Internet Access

Use Case: VDI zu ZIA (Internet)

Multisession non-persistent VDI (User Zuweisung über Pool)

On-Premise oder Public Cloud

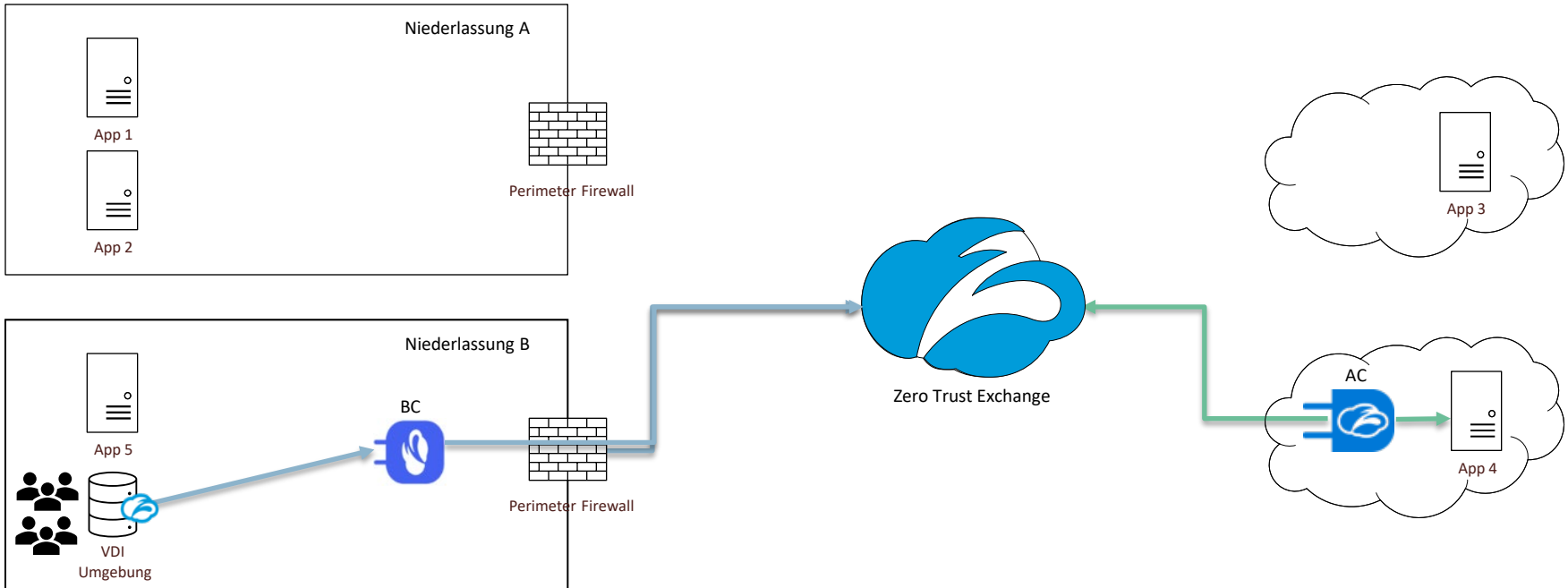


Use-Case - VDI zu Private Access

Use Case: VDI zu ZPA (App 4)

Multisession non-persistent VDI (User Zuweisung über Pool)

On-Premise oder Public Cloud





Vorteile von Zero Trust SD-WAN im Überblick

Vorteile Cloud und Branch Connector

Zero Trust für gesamten Traffic

- Für User, Geräte, Server sowie IoT/OT
- Unabhängig ob On-Premise oder Cloud

Einfache Architektur

- Ersatz für Site-to-Site VPNs oder MPLS-Netzwerk durch direkte und sichere Cloud-Verbindung
- Hybride Architektur möglich mit bestehender SD-WAN Umgebung

Geringe Angriffsfläche durch Zero Trust

- Private Applikationen nicht erreichbar aus dem Internet
- Nur direkte Verbindung zu Applikationen und nicht dem Netzwerk

Sichere IoT- und OT Verbindungen

- Erkennung und Klassifizierung von IoT-Geräten anhand von Traffic-Profilen
- Sichere & Clientless Browser-basierte Zugriffe auf OT-Systeme (SSH/RDP/VNC)

Zentrale Policies

- Granulare Forwarding Policies für ZIA- und ZPA-Traffic
- Policies für ähnliche Standorte auch möglich (z.B. mehrere Branches)



Offene Fragerunde & Diskussion

Offene Fragerunde & Diskussion

Fragen in die Runde:

- Welche konkreten Use-Cases sehen Sie aktuell oder zukünftig für den Einsatz von Branch- oder Cloud-Connectoren in Ihrem Unternehmen?

Offene Fragerunde & Diskussion

Fragen in die Runde:

- Vor welchen Herausforderungen stehen Sie typischerweise bei der Integration neuer Standorte oder im Rahmen von M&A-Projekten?