AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

IT-Security Deep Dive

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Zero Trust Branch (ZTB) mit Airgap – wozu ist das gut?

René von Arx
Principal Security Engineer,
AVANTEC

Raffael Späni
Senior Security Engineer,
AVANTEC

Rahmen der technischen Session

AVANTEC
Competence. Security. Trust.

- Vorstellungsrunde (Name, Firma: max 5 min)
- Wie kann man ZTB einordnen, wo macht es Sinn (10 min)
- Welche spannende Eigenschaften / Neuerungen gibt es bei Zscaler im Bereich ZTB mit Airgap (10 min)
- Kurzdemo ZTB. (10 min)
- Offene Runde (10 min)
  - Fragen & Antworten
  - Eigene Anforderungen an ZTB

Ziele der Session

AVANTEC
Competence. Security. Trust.

1. Spannende Neuerungen / Eigenschaften bei ZTB aufzeigen
2. Anwendungsbeispiele & Use-Cases kennenlernen, um eigene Einsatzmöglichkeiten zu identifizieren
3. Möglichkeiten zur einfachen Integration im bestehenden Setup erkennen
4. Erfahrungen austauschen durch eine Diskussion & offene Fragen klären
5. Informationen zur Verfügung stellen für die Tiefe (die Zeit reicht dafür nicht)
6. Sie wissen wo sie sich für «mehr» melden können

Agenda

AVANTEC
Competence. Security. Trust.

- Motivation
  - was bringt es , MPLS, SD-WAN, VPN, Site-to-Site-VPN,Teil-FW, Merger usw
- Möglicher Kunde
- Konzept des ZTB
  - Traffic für ZCC, Server und IoT
- Airgap
- Ausblick -> Raffael Späni geht an die Zenith für mehr
- Demo
  - ZT-400 (VM auf VMWare Workstation)
  - Client / Server
  - IoT -> Versuch mit Webcam wegen Zeitmangel nicht priorisiert
- Fragen & Antworten
- Diskussion
- Nützliche Links

AVANTEC
Competence. Security. Trust.

Wir sorgen für höchste IT-Sicherheit –

was uns dabei wichtig ist.

Wer ist wer?

- Wie heissen Sie?
  - René von Arx
- Bei welcher Firma arbeiten Sie?
  - AVANTEC AG seit 16 ¾ Jahren; knapp 15 Jahre Zscaler
- Welches ist Ihre Aufgabe?
  - Teamlead Content Security, vormals Zscaler ZIA PM der AVANTEC

- Wie heissen Sie?
  - Raffael Späni
- Bei welcher Firma arbeiten Sie?
  - AVANTEC AG seit 11 Jahren; so lange Zscaler
- Welches ist Ihre Aufgabe?
  - Senior Security Engineer, Technische PM-Rollen in der AVANTEC

AVANTEC
Competence. Security. Trust.

Damit Gefährliches draussen bleibt –

wer sich dafür auf uns verlässt.

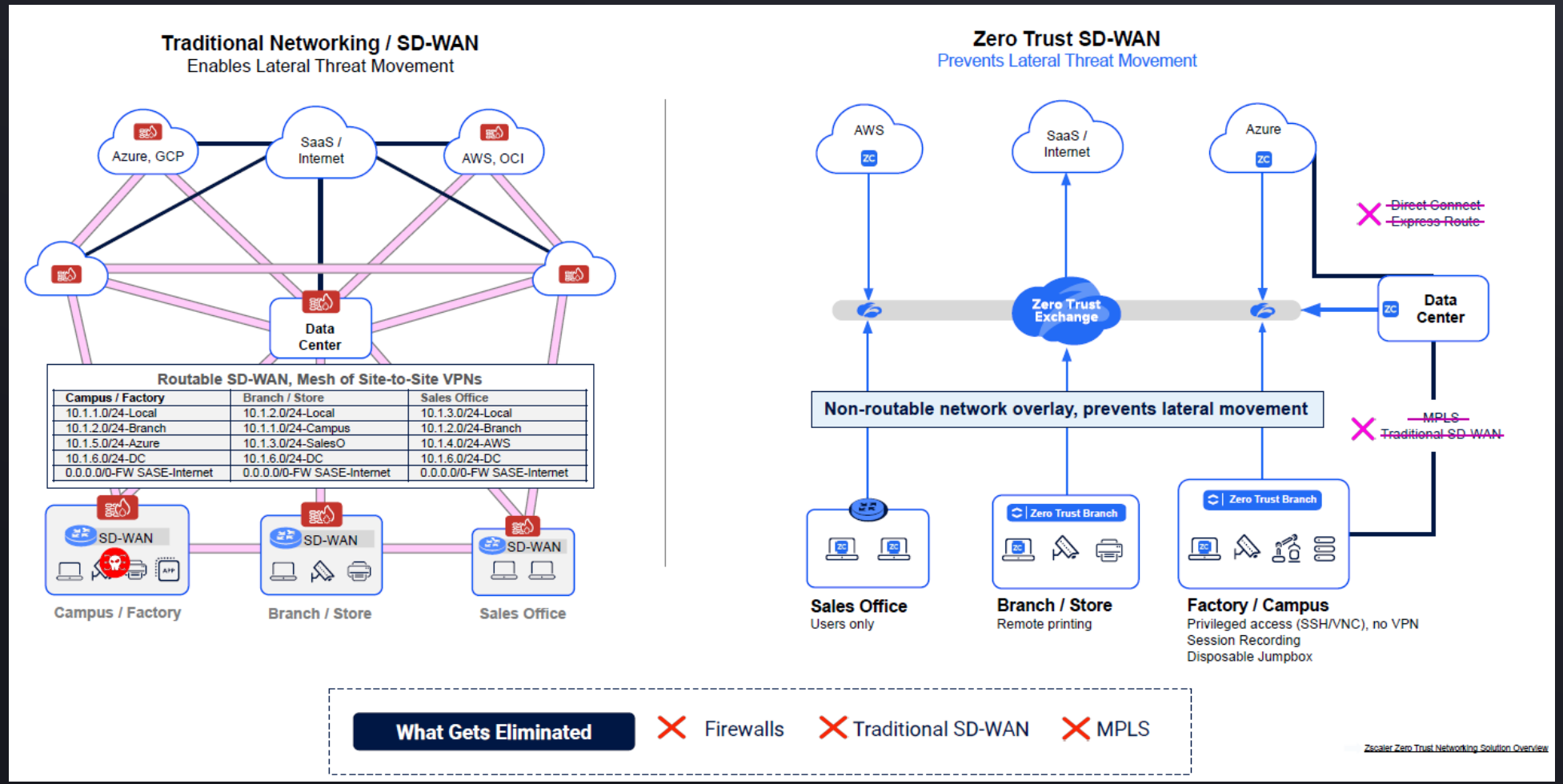
Motivation

Gründe zusammengestellt

- Konsolidieren vom Netzwerk und der Security in eine Platform
- Schnelleres Onboarding durch gleichen/ähnlichen Setup
- Reduktion oder Eliminierung von VPNs, MPLS-Leitungen und (Teil)-Firewalls
- Segmentierung der einzelnen Devices (Airgap) oder Devicegruppen (Airgap Lite oder Plus)

- Wie ein Kaffeeshop in der Branch
- Beschleunigte Merger & Aquise
- Zero Trust Fabrik mit Produktionsmaschinen uwm

Motivation – Absichern externe Kommunikation



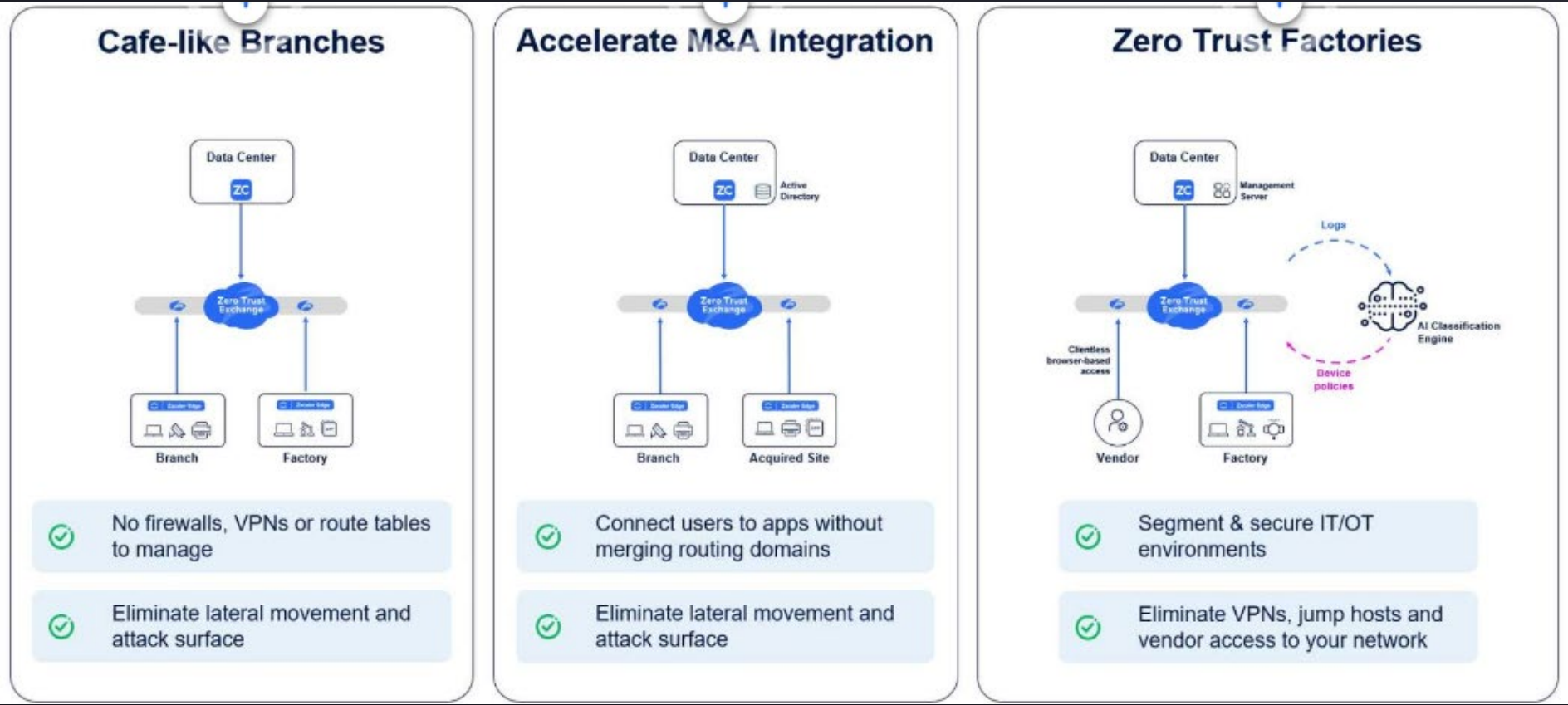
Motivation - Beispiele

IPSec für ZIA

Firewall minimal

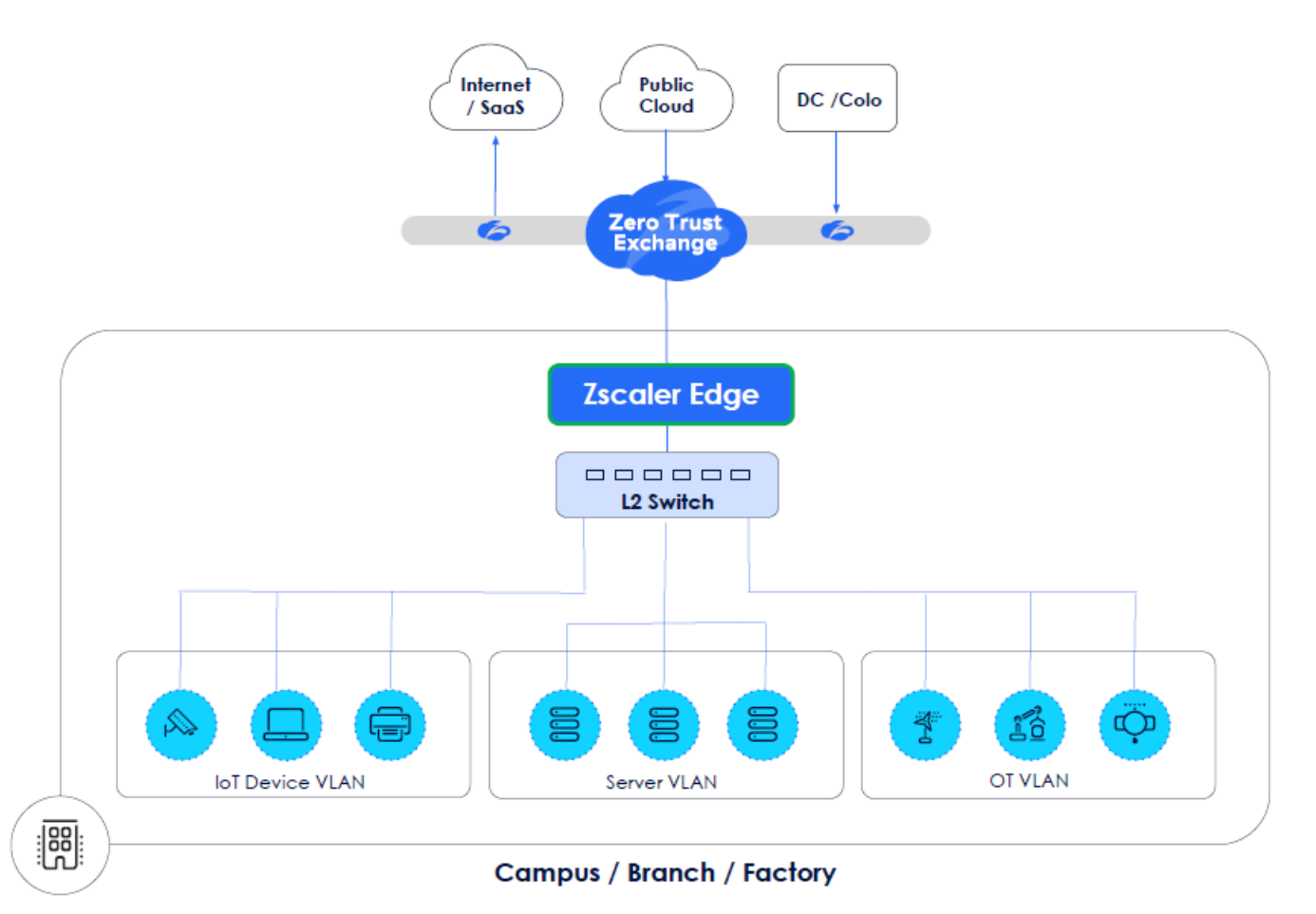
Keine IP-Ranges verwenden

App Connector aktiv



Motivation - Segmentierung

Unified Appliance ZT-SDWAN + ZT Device Segmentierung => ZTB



Zero Trust Exchange

L2 Switch mit dot1q
VLAN Tagging
oder
ohne Tagging (VLAN 1)

Trennung durch
physischen Port
oder
VLAN

Je nach Hardware bis
20 ZT-400 und bis 40 ZT-600/800 VLAN auf dem Trunk

Möglicher Kunde

Beispiel 1

Cornerstone Building Brands

Largest manufacturer of exterior building products in North America

Over 19,000 employees and 180 sites globally

HQ: Cary, NC

Industry: Manufacturing

CORNERSTONE BUILDING BRANDS

- Driving digital transformation across IT & OT to improve business agility
- Eliminated multitude of point products with **Zero Trust Branch** for offices & factories
- Simplified vendor access to OT systems with **Privileged Remote Access**

Products: Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Zero Trust SD-WAN, Privileged Remote Access

Problem

Growth through acquisitions: Cornerstone has grown significantly through multiple acquisitions, leading to a complex sprawl of disparate factories, offices and IT systems.

Slow M&A integration: Integrating new sites and users took 9-12 months, delaying value realization.

Vendor Remote Access: Third-party access to OT systems was complex and expensive, requiring unsafe VPN access in some cases, and physical site visits in other cases.

Solution

Zero Trust for Users, Branches, Factories: Cornerstone adopted a zero trust architecture for users and locations to ensure a consistent café-like experience from anywhere

Privileged Remote Access: Cornerstone adopted Zscaler Privileged Remote Access for vendor remote access into OT systems, eliminating VPNs, lateral movement risk and expensive site visits

Benefits

Faster M&A integration: Using a zero trust architecture, Cornerstone reduce M&A integration times from 12 months to **60 days**

Reduces Cost & Complexity: With Zero Trust Branch, Cornerstone eliminated reliance on VPNs, reduced operational costs and avoided expensive site visits for third-party technicians.

Reduced Risk: Cornerstone eliminated third-party risk from VPNs and ensured safety & uptime for their factories

Problem
- Mehrere Zukäufe
- Dadurch langsame Integration
- 3rd-Party Zugriff auf OT

Lösung
- ZTB
- ZPA PRA

Vorteile
- Schnellere Integration
- Reduktion der Kosten, Komplexität und Risiken

Möglicher Kunde

Beispiel 2

Kingston Technology

Kingston Technology is a world leader in memory products and technology solutions, trusted by leading PC manufacturers and cloud providers around the world.

3,000+ employees, 63+ Surface Mount Technology (SMT) lines

HQ: Fountain Valley, UK

Industry: High-tech

Kingston TECHNOLOGY

- Secured **internet and private application access** through the Zero Trust Exchange
- Extended zero trust to the factory floor with **OT/IoT segmentation**
- Completed segmentation and **achieved compliance** without taking machines offline

Products: Internet Access (ZIA), Private Access (ZPA), OT/IoT Segmentation

Problem

Legacy approach to segmentation made it **complex to provision and manage** policies for the 90 types of devices on Kingston Technology's factory floor, including thermal units, packaging machines, testing machines, manufacturing line equipment

Mis-provisioned access increases **risk exposure** for OT assets

Solution

Secured access to the internet and private applications with the Zero Trust Exchange, including Zscaler Internet Access and Zscaler Private Access

Extended zero trust to the factory floor with OT/IoT Segmentation, where every device is secured without taking endpoints offline and without the need for agents, east-west firewalls, or VLAN readdressing

Benefits

Reduces complexity and risk by enforcing policy on every endpoint, with the granularity to control.

Applies segmentation in minutes and without taking devices offline, unlike in legacy approaches where making policy changes means days of offline devices and delays to the factory line

Problem
- Segmentierung, alter Ansatz zu komplex
- Hohes Risiko

Lösung
- ZPA / ZIA
- ZTB für IoT und OT in der Fabrik

Vorteile
- Reduktion der Komplexität und Risiken
- Segmentierung in Minuten

Konzept ZTB

Appliance Optionen – Stand Q4/25

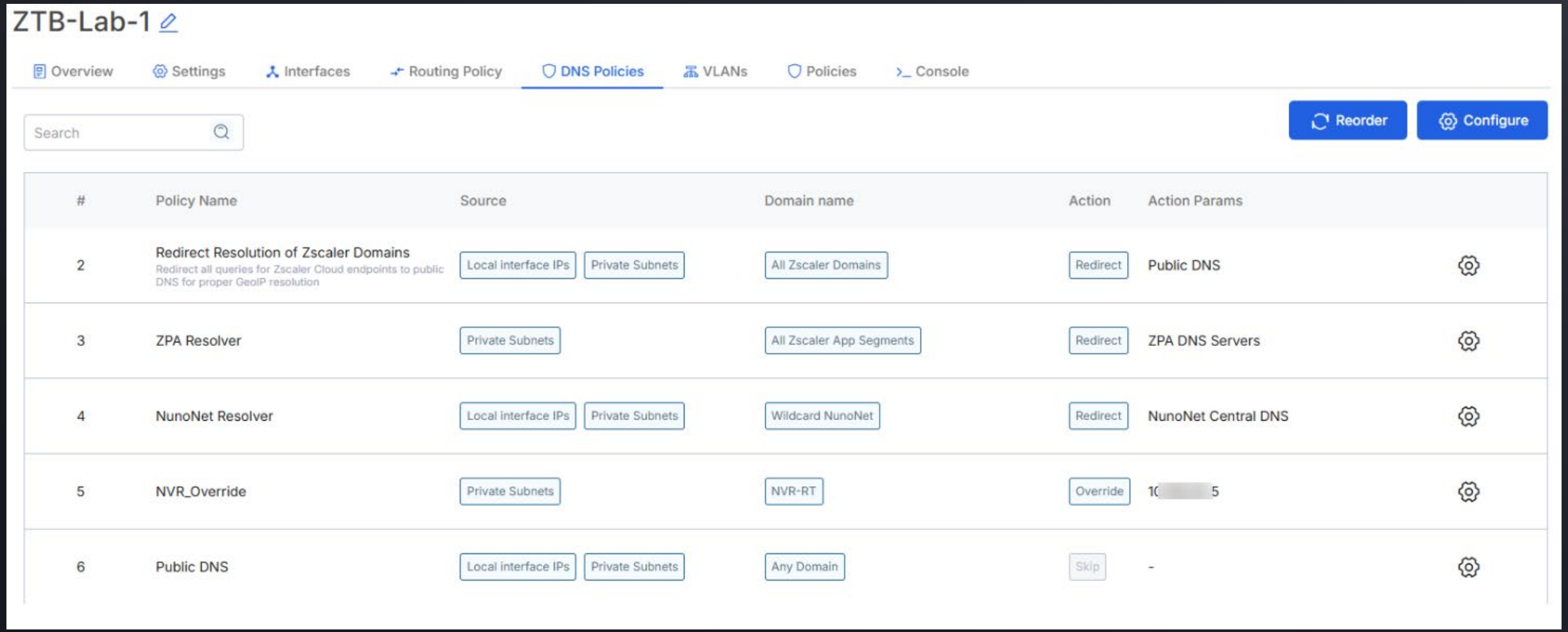
AVANTEC
Competence. Security. Trust.

	ZT400	ZT600	ZT800	ZT8010	VM
CPU	4C Atom	4C Atom	8C Atom	16C Xeon	2 to 8 vCPUs
Memory	16GB DDR4	16GB DDR4	32GB DDR4	128GB DDR4	8 to 32GB
Storage	512GB	512GB	512GB	1TB	256GB
Ports	4x 1GbE	6x 1GbE	6x 1GbE 2x 1GbE (SFP)	10x 1GbE 8x 10 GbE	4 vNICs
Form Factor	Desktop	Desktop	Desktop	1U	VM
Other Features	**Fanless**	**-**	**-**	**Dual PSU**	**-**
Throughput (Unencrypted)	**2 Gbps**	**2 Gbps**	**5 Gbps**	**40 Gbps**	**20 Gbps**
Throughput (Encrypted)	**200Mbps**	**400Mbps**	**1 Gbps**	**5-10 Gbps**	**1 Gbps**
# Endpoints	**200**	**200**	**1000**	**5000**	**1000**

Konzept ZTB

Granulare Kontrolle – DNS Policy

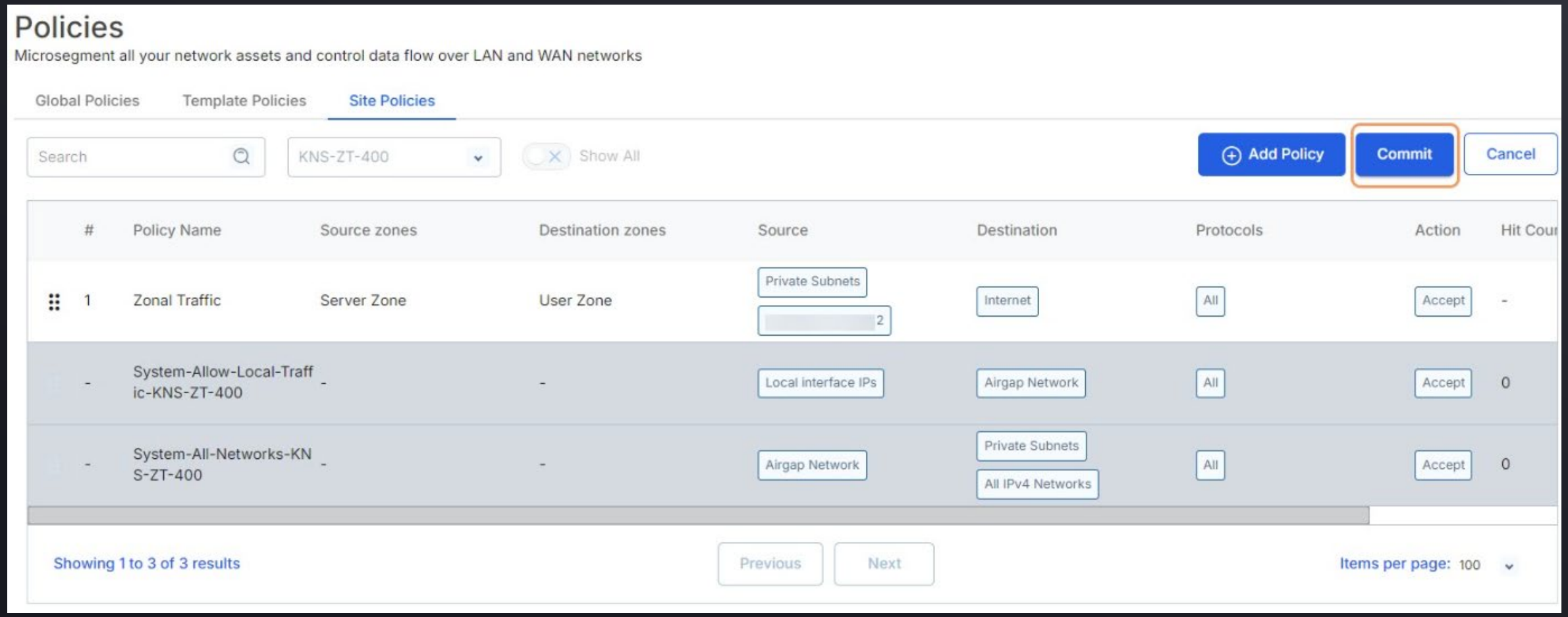
AVANTEC
Competence. Security. Trust.



Konzept ZTB

Granulare Kontrolle – Firewall Policy

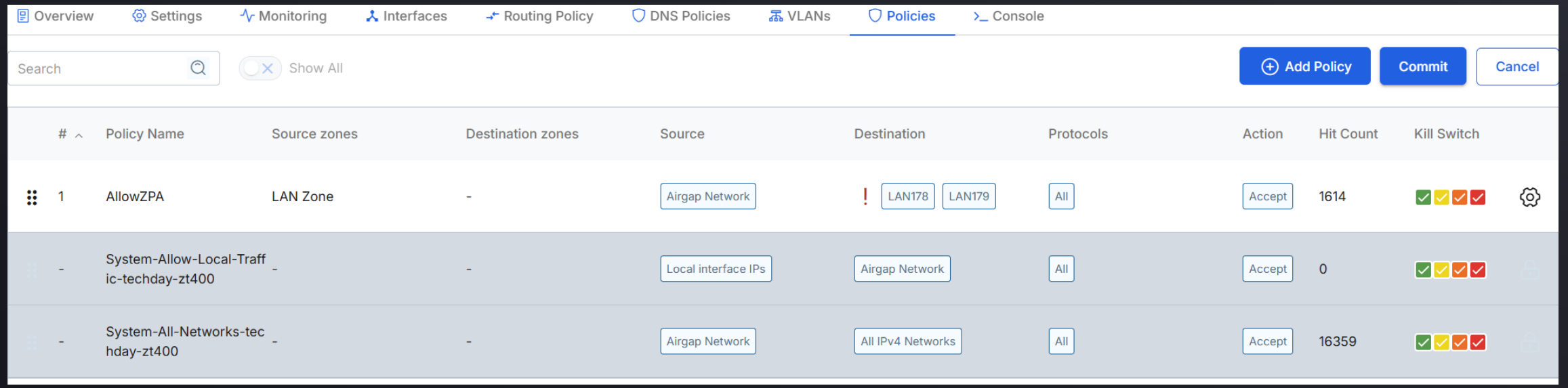
AVANTEC
Competence. Security. Trust.



Konzept ZTB

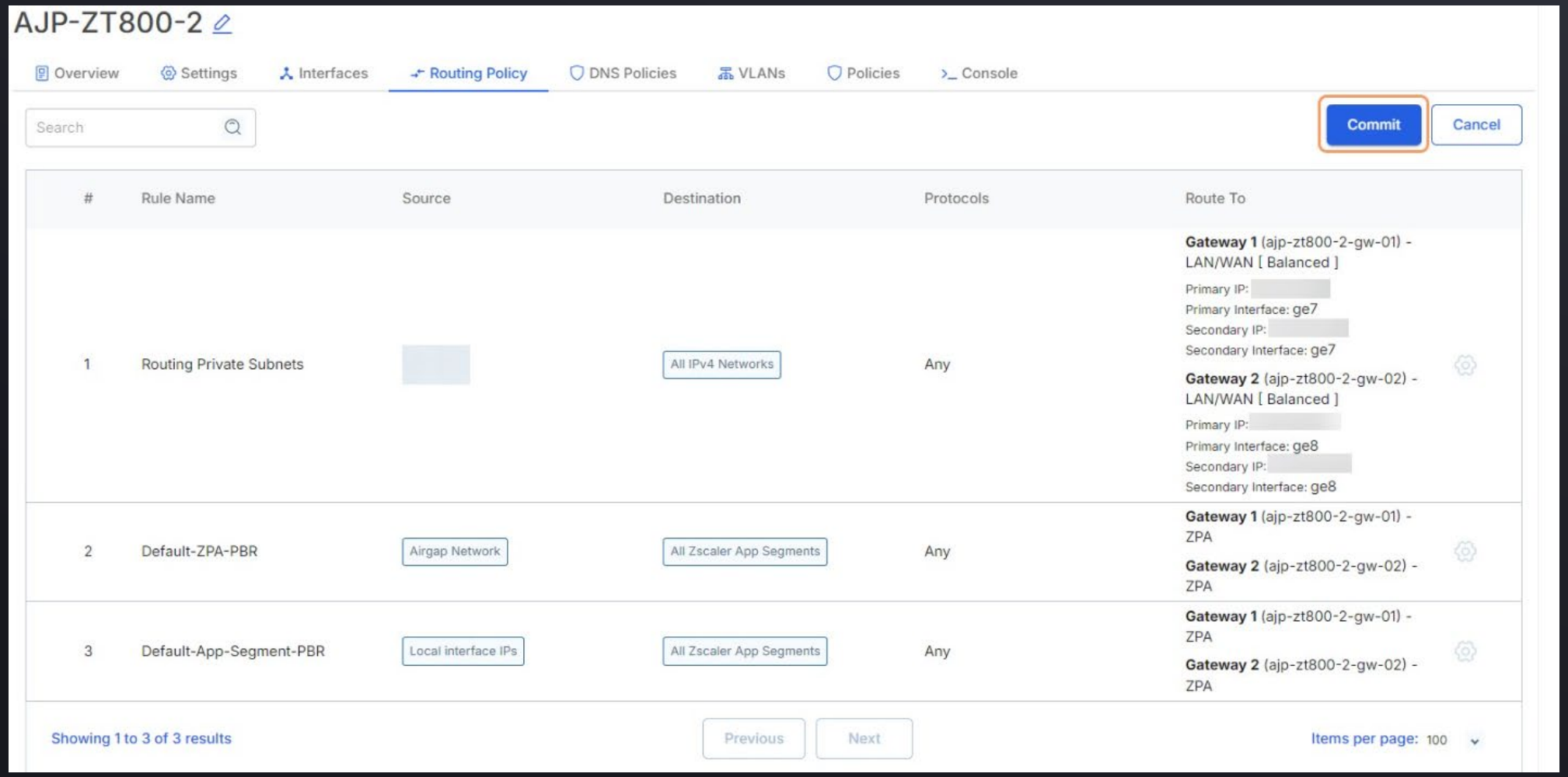
Granulare Kontrolle – Firewall Policy mit Kill Switch

AVANTEC
Competence. Security. Trust.



Konzept ZTB

Granulare Kontrolle – Routing Policy

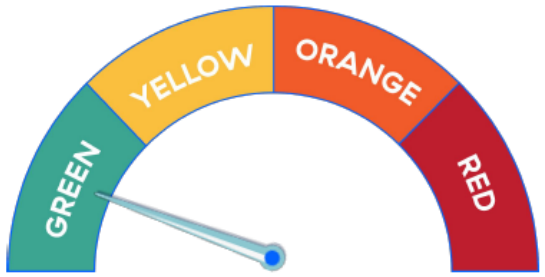


Konzept ZTB

Granulare Kontrolle – Ransomware Kill Switch

https://help.zscaler.com/zero-trust-branch/understanding-ransomware-kill-switch

Incident response tool surgically stops lateral propagation



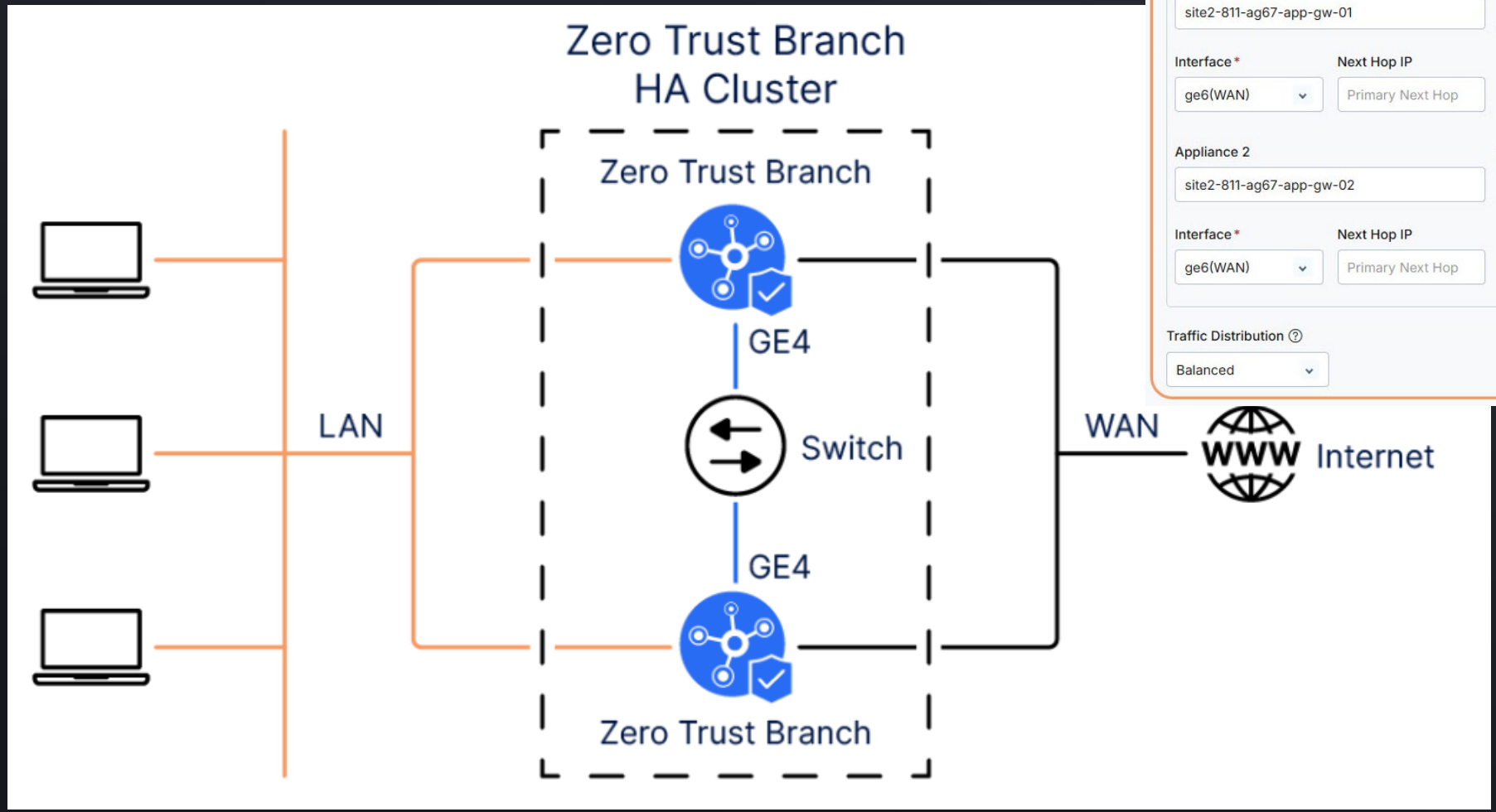
Reduce attack surface during triage

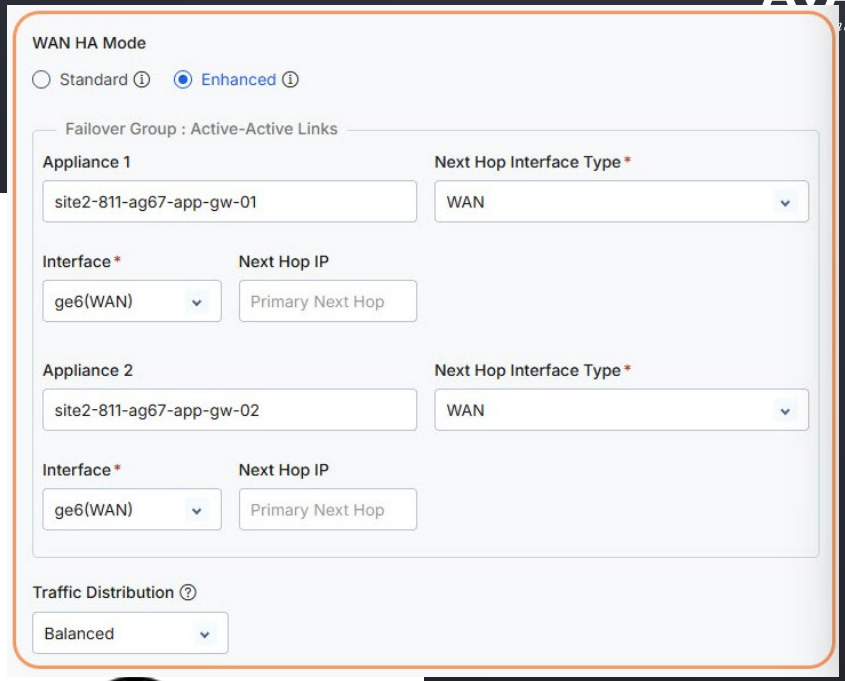
Maintain business operations with tiered response policies

1	Allow-SMB	Users	Servers	tcp:445 tcp:137 tcp:139	Accept	0	
2	Allow-RDP	Server Admins	Servers	tcp:3389	Accept	0	
4	Allow-SSH-OT	OT Admins	OT Devices	tcp:22	Accept	0	
5	Allow-SSH-OT	Block-all	OT Devices	All	Drop	0	

Konzept ZTB

HA Cluster – wir gehen in dieser Session nicht darauf ein.





AVANTEC
Competence. Security. Trust.

Damit Security Know-how immer verfügbar ist –

wie wir Lücken schliessen können.

Airgap

Was kann es etwas allgemeiner

- Ausweitung von Zero Trust auf Geräte in internen Netzwerken
  - Networks garantiert die Einhaltung von Zero Trust-Prinzipien für den Ost-West-Datenverkehr von Geräten im LAN.
  - Die interne Angriffsfläche lässt sich durch die Eingrenzung der lateralen Verbreitung von Bedrohungen in Campus- und OT-Netzwerken eliminieren.
- Sicherung kritischer OT-Infrastrukturen
  - Bietet Geräteerkennung in Echtzeit und Inline-Durchsetzung. Sie fungiert als Ransomware-Kill-Switch, da die nicht notwendige Kommunikation von Geräten deaktiviert und damit eine laterale Ausbreitung von Bedrohungen gestoppt wird, ohne den Geschäftsbetrieb zu unterbrechen. Die Lösung von Airgap Networks neutralisiert moderne Bedrohungen wie Ransomware für IoT-Geräte, OT-Systeme und Geräte, auf denen keine Agenten eingesetzt werden können.
- Vereinfachter Betrieb und Kosteneinsparungen
  - Macht risikoanfällige Ost-West-Firewalls und veraltete Sicherheitstechnologien wie Network Access Control (NAC) überflüssig, da sie den gesamten Datenverkehr von verwalteten und nicht verwalteten Geräten in jedem Niederlassungs-, Campus- oder Fabriknetzwerk identifizieren und kontrollieren kann, ohne dass Änderungen an der bestehenden Switching- und Routing-Infrastruktur erforderlich sind. Dies verbessert die Sicherheitslage von Unternehmen deutlich, da herkömmliche NAC-Ansätze mit dem Grundprinzip von Zero Trust “never trust, always verify” nicht in Einklang zu bringen sind.

Airgap

Hauptmerkmale und Vorteile von Zscaler Airgap

- Agentenlose Mikrosegmentierung
  - Schützt Geräte, auf denen keine Software installiert werden kann (z. B. IoT, Produktionsmaschinen, Server), ohne Unterbrechung des Betriebs.
- Segment-of-One Architektur
  - Jedes Gerät wird in sein eigenes isoliertes Segment gestellt, was direkte Kommunikation zwischen Hosts (laterale Bewegung) verhindert. Mit DHCP Proxy.
- Identitätsbasierte Richtlinien
  - Durch die Nutzung von Telemetriedaten werden detaillierte Kontrollen angewendet (ähnlich einer Host-ACL), um nur notwendigen Datenverkehr zu erlauben.
- Schutz von OT-Umgebungen
  - Ideal für Fabriken und kritische Infrastrukturen, um Legacy-Systeme abzusichern.
- Reduzierung von Komplexität
  - Ersetzt oft die Notwendigkeit für traditionelle, komplexe interne Firewalls und NAC-Lösungen (Network Access Control).
- Transparenz
  - Bietet Einblick in autorisierte und nicht autorisierte Geräte und visualisiert Kommunikationsmuster im Netzwerk.
- Baut auf ZIA und ZPA auf
  - Regelwerk kann weiter verwendet werden.

Airgap Mode

Welche «Protection Soutions» sind verfügbar

- Airgap-Lite
  - Behavior: Uses the same subnet mask as the one the DHCP server provides, which simplifies integration in environments where endpoints need to communicate directly without routing all traffic through the gateway.
  - Use Case: Suitable for systems or networks where full isolation is not a strict requirement.
  - Trade-Off: Reduces isolation as compared to Airgap.
- Airgap
  - Behavior: Assigns a /32 network mask to endpoints, giving each device its own unique IP address and enabling admins to enforce device-level isolation. Admins can use firewall policies to explicitly prevent direct communication between hosts and effectively create a secure "network of one."
  - Use Case: Ideal for environments that require complete isolation between endpoints, ensuring all traffic routes through the Zero Trust Branch appliance for inspection and enforcement.
  - Challenge: Some systems might not support /32 masks due to hardware or software limitations. In such environments where the /32 subnet mask is not supported, the admins can choose Airgap+ or Airgap-Lite (if full isolation is not a strict requirement) mode.

Airgap Mode

Welche «Protection Soutions» sind verfügbar

- Airgap+
  - Behavior: Implements micro-subnets by supporting subnet masks between /27 and /30. Devices within the same micro-subnet can communicate directly without routing through the Zero Trust Branch appliance. Traffic between different micro-subnets or external destinations is routed through the gateway for inspection and enforcement.
  - Use Case: Provides a balance between complete isolation and full subnet communication, which is ideal for environments needing some level of local communication while still enforcing Zero Trust Branch policies for external traffic.
  - Trade-Off: Adds configuration and maintenance complexity as multiple subnets are managed.

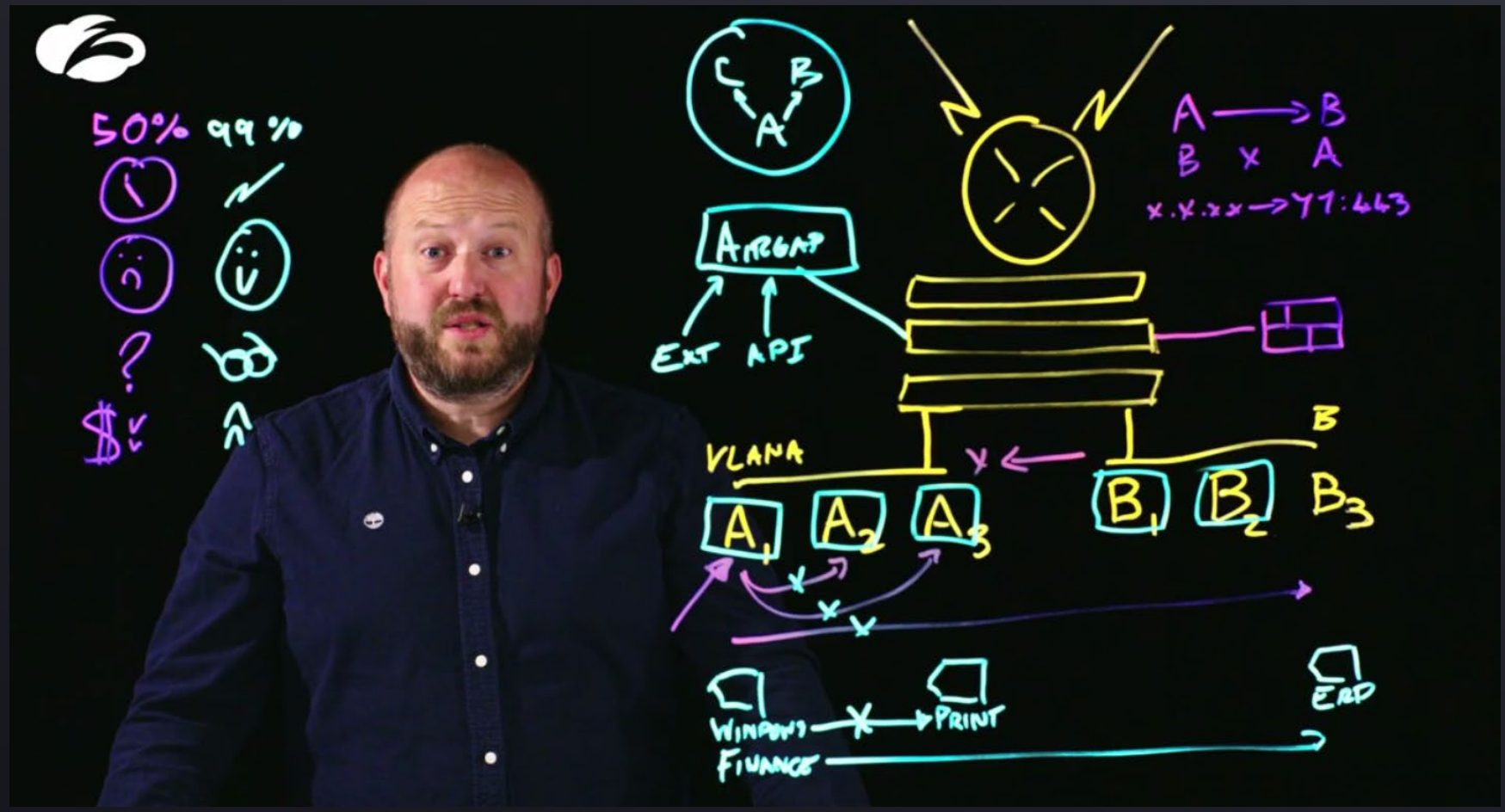
  Requirements:
  - The Zero Trust Branch appliance must operate in server mode for the associated VLAN(s).
  - Available starting with Airgap OS 7.7.6. (aktuell 8.0.5/8.0.8)

Airgap

Warron erklärt https://www.youtube.com/watch?v=g2AoyG82XEc

- Gelb: bestehende Umgebung
- Violett: bestehende Lösungen anderer Hersteller ; auch FW-basiert.
- Blau: Zscaler Funktionalität

- Airgap Microsegemntierung
  - Kein lateral Movement
  - Kurzfristig unterbinden von zB printen, aber EAD-Zugriff bleibt (Dokumente)



Demo

Allgemein

AVANTEC
Competence. Security. Trust.

- VM ensteht aus einem ISO
- Alte HW aus Portal entfernen und ISO aufspielen; neuen AuthCode erstellen
- Spezialfall ZT-400 mit Fehlertoleranz bezüglich Setupwechsel
- Heikel bezüglich OS und ESXi Version
  - Wir haben auf einer ESXi 6.7 ein vmdk erzeugt, welches dann per ovf importiert werden kann
  - Läuft nun auch bei uns auf Proxmox (qemu)
- Läuft auch auf VMWare Workstation; aus vmdk einfach zu erstellen
- Restricted Shell ohne Root-Rechte und zwei verschlüsselten Partitionen.
- Installation erst nach Setup und Reboot.
- Docker basiert
- Etwas Reverseengineering gemacht (Installscript zB)

- Zeigen GUI
- Linuxserver über ZIA
- IoT

Demo

Mein Setup Teil I

techday-zt400	zt400-techday-single	AVALAB-BTEST-01	techday-zt400-gw-st	Standalone	192.168.52.251	8.0.5

- ZT-400
  - GE3 verbunden mit HTC Hotspot
  - GE2 192.168.253.0/24 Airgap inkl Airgap +
  - GE4 192.168.177.0/24 Airgap inkl Airgap +

Airgap VLAN	VLAN Tag	Interface-IP	Zone	Subnet/Mask	Features	Disable/Enable
vlam-177	1	ge4 - 192.168.177.1	LAN Zone	192.168.177.0/24	-	
vlan-253	1	ge2 - 192.168.253.1	LAN Zone	192.168.253.0/24	-	
wan-techday-zt400-gw-st	1	ge3 - 192.168.52.251	WAN Zone	192.168.52.0/24	-	

- ZIA über IPSec und ZPA über App Connector
- VLAN-253 : Raspberry Pi 4 mit Ubuntu Server und Apache2
  - Kein ZCC installiert
    - Curl ipinfo.io/ip https://ip.zscaler.com
    - Vom Browser auf https://192.168.253.41

Demo

Mein Setup Teil II

AVANTEC
Competence. Security. Trust.

- Dashboard Insights -> Raspberry
- Assets
- Sites Techday-zt400
  - Settings ZIA IPSec
  - ZPA
  - Monitor
  - Interfaces
  - Console
    - tail /var/log/syslog
- Monitoring & Logs
  - Packet Logs
  - Flow Logs

- screen /dev/ttyUSB0 115200 (CTRL a d)

Demo

Mein Setup Teil III

```
+-----------------------------------------------------------+
|                                                           |
|                  Airgap Networks Gateway                  |
|                                                           |
|                    techday-zt400-gw-st                    |
|                        (Standalone)                       |
|                                                           |
|-----------------------------------------------------------|
|    1 - Configure Gateway                                  |
|-----------------------------------------------------------|
|    2 - Change Administrator Password                      |
|    3 - Show Configuration                                 |
|    4 - Show Gateway Status                                |
|-----------------------------------------------------------|
|    5 - Troubleshooting                                    |
|    6 - Platform CLI                                       |
|    7 - Version                                            |
|    8 - Exit                                               |
|                                                           |
|    Management System: https://avavonarx.goairgap.com     |
|                                                           |
+-----------------------------------------------------------+
SELECT> |
```

```
Gateway State : Standalone

WAN Connectivity:
Checking Default Gateway(192.168.52.1) ...OK
Checking reachability to internet...OK
Web Proxy is not configured.
Checking Management Portal reachability...OK
Checking Analytics connection...OK
Checking Debug Port reachability...OK

Services Status:
Service                         State
Network Poller                  active (running) since Tue 2026-05-05 06:50:03 UTC; 23h ago
DHCP Server                     active (running) since Tue 2026-05-05 09:12:55 UTC; 21h ago

Network Status:
NAMES                IMAGE                                                  STATUS
kinesis              docker.repos.goairgap.com/7-8/kinesis:1.2              Up 22 hours
dnsproxy_container   docker.repos.goairgap.com/7-8/dnsproxy:8.0.5           Up 24 hours
strongswan           docker.repos.goairgap.com/7-8/strongswan:latest        Up 24 hours
policy_container     docker.repos.goairgap.com/7-8/poller:8.0.5             Up 24 hours
zeek                 docker.repos.goairgap.com/7-8/zeek:asset_discovery_241210  Up 24 hours
vyos_container       docker.repos.goairgap.com/7-8/vyos:1.4.4-sagitta       Up 24 hours
techday_ac_zt400     zscaler/zpa-connector:latest.amd64                     Up 24 hours

Press [Enter] to continue |
```

Resumé

AVANTEC
Competence. Security. Trust.

- Klein starten
- Labor ohne HA, dann mit HA
- Nicht jeden Upgrade mitmachen, wenn alles läuft
- Vorher Architektur gut überlegen und planen
- Sizing gut überlegen
- Genug Zeit einplanen bei den ersten Standorten um Erfahrungen zu sammeln
- Laufende Verbesserungen und es geht in die richtige Richtung
- Wenn vorhanden mit ESXi starten

Fragen & Antworten & Diskussion

AVANTEC
Competence. Security. Trust.

- Wer hat ZTB im Einsatz?
- Wer plant ein Projekt?
- Wer wurde nun überzeugt, das in Angriff zu nehmen?

- Gerne unterstützen wir Sie dabei

Anhang

Nützliche Links

AVANTEC
Competence. Security. Trust.

- RBAC (Super Admin, Network Admin, Security Admin, Viewer)

  https://help.zscaler.com/zero-trust-branch/understanding-zero-trust-branch-access-roles
- Objects

  https://help.zscaler.com/zero-trust-branch/about-objects
- Tags

  https://help.zscaler.com/zero-trust-branch/working-with-tags
- Assets

  https://help.zscaler.com/zero-trust-branch/managing-your-assets
- Templates (grosse Umgebungen)

  https://help.zscaler.com/zero-trust-branch/managing-templates
- Routing Policies (ZIA ZPA Internet)

  https://help.zscaler.com/zero-trust-branch/understanding-routing-policies
- DNS Policies

  https://help.zscaler.com/zero-trust-branch/what-site-dns-policies
- Configure VLAN

  https://help.zscaler.com/zero-trust-branch/configuring-vlan

Nützliche Links

AVANTEC
Competence. Security. Trust.

- Ransomware Kill Switch (Zscaler Demo)

  https://help.zscaler.com/zero-trust-branch/understanding-ransomware-kill-switch

AVANTEC
Competence. Security. Trust.

Wir sorgen für höchste IT-Sicherheit –

was uns dabei wichtig ist.

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

DANKE

BeyondTrust · CHECK POINT · CROWDSTRIKE · digicert · netskope · THALES · tenable · xorlab · zscaler

AVANTEC
Competence. Security. Trust.

Nächste Session 13:00

Session 2

Was ist PAM mit Zero Standing Privileges (ZSP)? — Frei, 4. OG

Produkt: BeyondTrust
Referenten: Michael Scherzinger, Jessica Warland

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security — Odermatt, 4. OG

Produkt: zscaler
Referent: Jonas Kugler

Disaster Recovery im Cloud-Zeitalter — Lehmann Steingruber, 5. OG

Produkt: zscaler
Referent: Matthias Geiser

How to secure AI – Ein strategischer Überblick — Cancellara, 4. OG

Produkte: Diverse
Referent: Georg Hegyi

AVANTEC
Competence. Security. Trust.

Nächste Session 16:00

Session 4

Was ist PAM mit Zero Standing Privileges (ZSP)? — **Frei, 4. OG**

Produkt: BeyondTrust
Referenten: Michael Scherzinger, Jessica Warland

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security — **Cancellara, 4. OG**

Produkt: zscaler
Referent: Jonas Kugler

How to deploy Check Ponit SASE in 30 minutes — **Holdener, 5. OG**

Produkt: CHECK POINT
Referent: Tobias Wälchli

Einblick ins Cyber Defence CenterPRA — **Odermatt, 4. OG**

Referent: Tobias Balschun