Zscaler zero Trust Branch

Speaker:

Kureli Sankar

About Kureli Sankar

Present

Principal Technical Product Specialist - Zero Trust Branch

Prior Experience

5+ years - Routing and SD-WAN Leader, Technical Marketing
5+ years - Technical Marketing Engineer (Security)
6+ years - TAC Engineer (Security)
CCIE Security #35505
Distinguished Speaker at tier 1 conferences

Areas of Expertise

FW, IPS, SWG, AMP, CASB, DNS-Security
Zero Trust SD-WAN Security solutions

Kureli Sankar

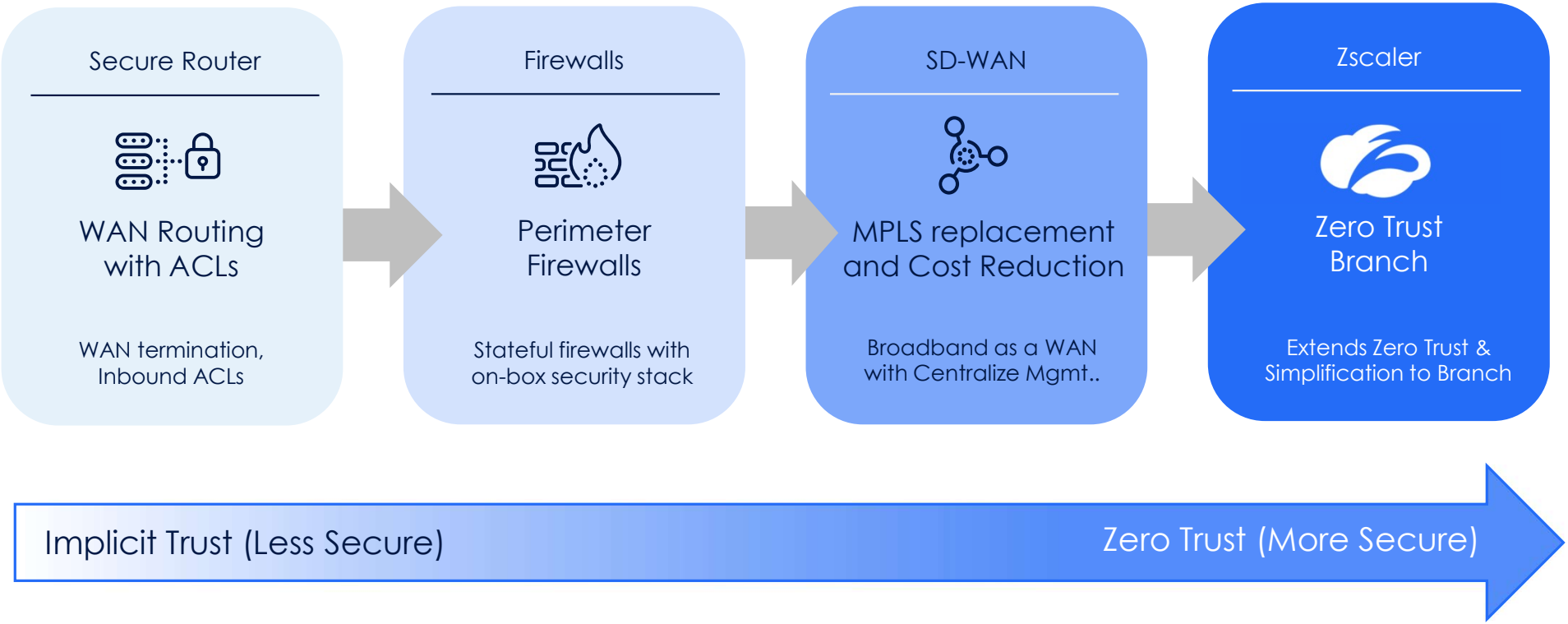
CISCO CCIE EMERITUS

Agenda

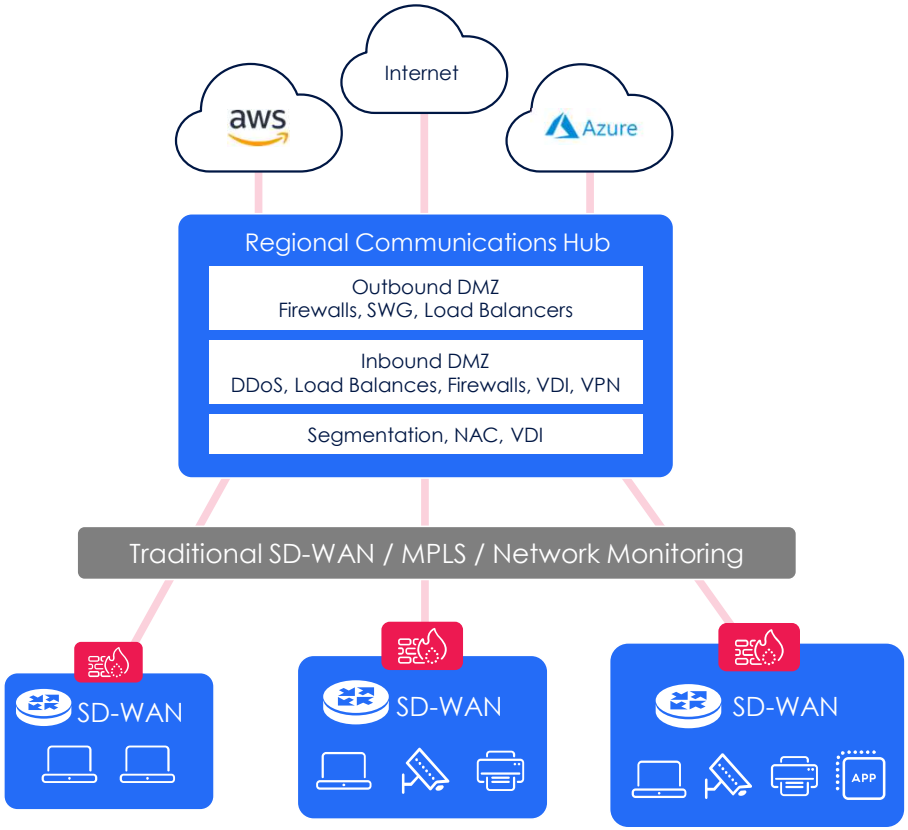
- Evolution of Branch and its Security Challenges
- Introducing Zscaler Zero Trust Branch and its Architecture
- Zero Trust SD-WAN Deep Dive
- Zero Trust Device Segmentation Deep Dive
- Zscaler Cellular
- Resources

Evolution of Branch

Zero Trust is the most effective security strategy against lateral threats



Traditional Networking and Security



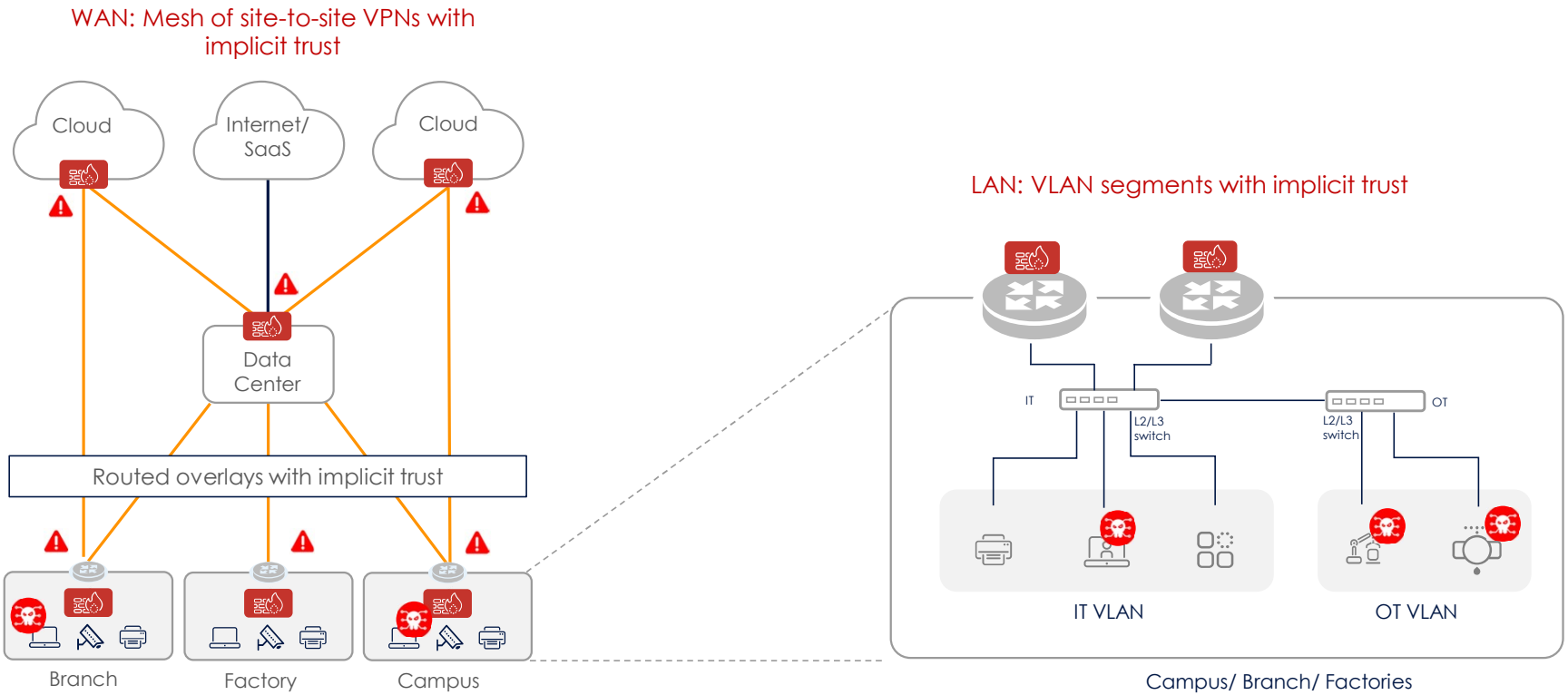
Enables lateral movement, facilitates ransomware attacks

Expands the attack surface, every internet firewall

Expensive and complex, routing & firewall rules

- N / S Firewalls, Internet
- N / S Firewalls, VPN
- E / W Firewalls, Segmentation
- Expensive Switches
- Privileged Remote Access

Legacy Architecture Inside Branch Enable Lateral Threats

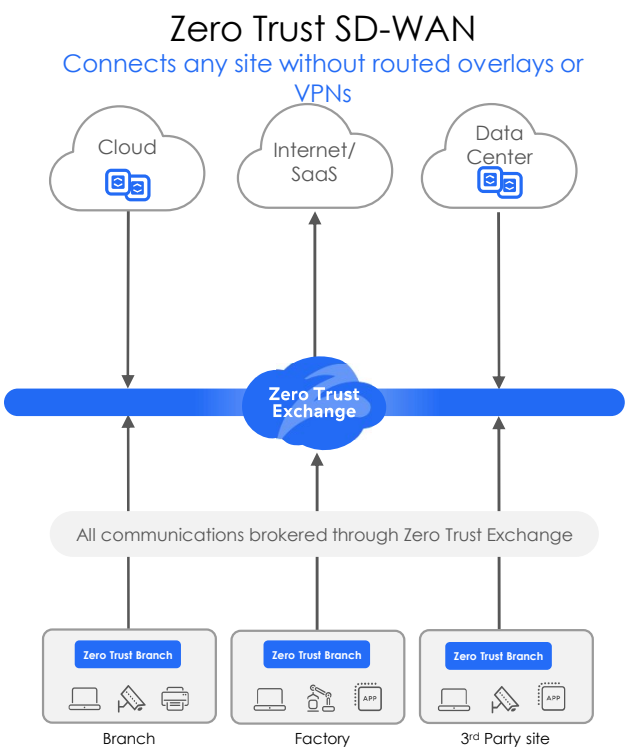


VLAN-based network segmentation is complex to manage

Policy exceptions, out-of-date policies and config errors leave security gaps, allowing ransomware to spread

Zscaler Zero Trust SD-WAN

Simplify and Secure External Communications



Secure Branch to Branch Connectivity via Zero Trust Exchange

- No overlay routing complexity
- No additional firewalls required
- Single policy engine for sites and users

More Secure

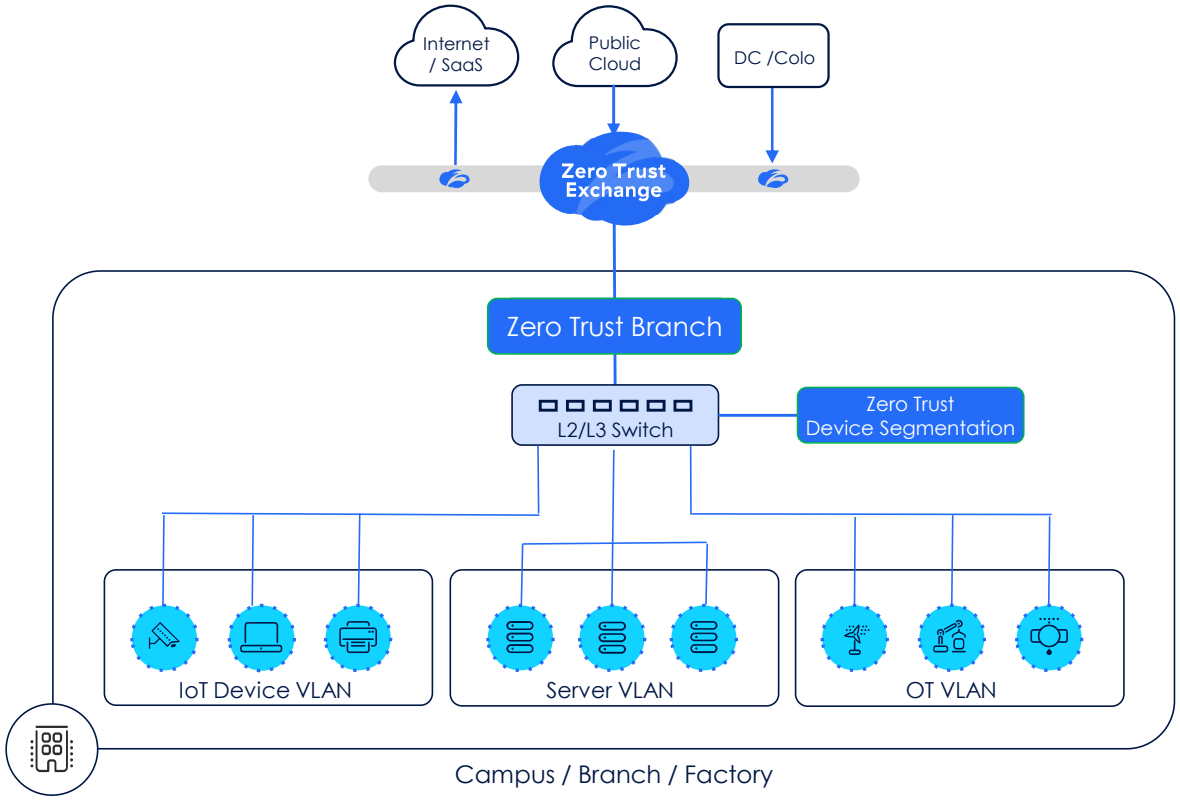
- Connects users and devices to apps through a brokered proxy
- Outbound only connections, eliminates the attack surface.

Simpler Management

- Granular forwarding policies for internet, SaaS and private apps
- No route tables to manage, no firewalls needed, no separate policies for users vs. devices

Introducing Zscaler Zero Trust Branch

Unified Appliance ZT SD-WAN + ZT Device Segmentation = Zero Trust Branch



- End lateral movement between and within branches, campuses, and factories
- Greatly simplify branch networking – eliminate firewalls, NAC, ACLs, site-to-site VPNs, ExpressRoute, Direct Connect, Route Propagation – All you need is an ISP connection
- Improve performance by providing direct app access, without backhauling to data centers

Zscaler Zero Trust SD-WAN

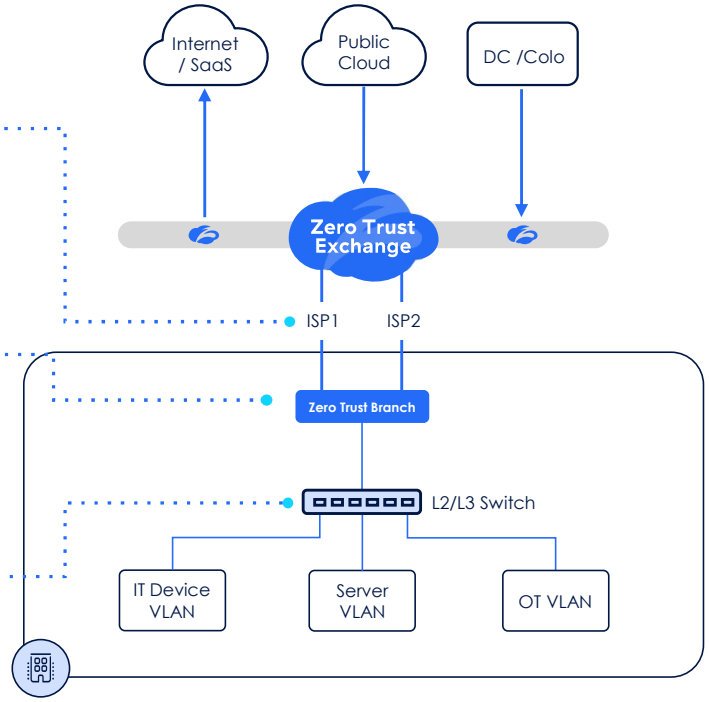
Zero Trust Branch: Edge Appliance

Secure outbound connectivity eliminates the attack surface and routing complexity

WAN Management
- multiple ISPs with monitoring
- policy based path selection
- connectivity to Zscaler ZTE
- static & optional dynamic routing

Integrated Gateway
- high availability
- integrated segmentation firewall
- Asset discovery, classification

LAN Interface Management
- multiple L3 LAN subnets
- 802.1q VLAN tagging
- DHCP Server / Relay
- DNS Gateway



Zero Trust Branch, Campus, or Factory

What Gets Eliminated

Networking
MPLS
Traditional SD-WAN

Inside the Branch
SD-WAN Routers
North – South Firewalls (Internet)
North – South Firewalls (VPN)

Key Differentiators

- No inbound IP ports exposed
- Reduced routed overlays, simplified connectivity and operations
- Built in Zero Trust; Lateral threat movement prevention

Zscaler Zero Trust SD-WAN – How It Works

Users and Devices Connect to Applications, Not Networks (Eliminates Network Implicit Trust)

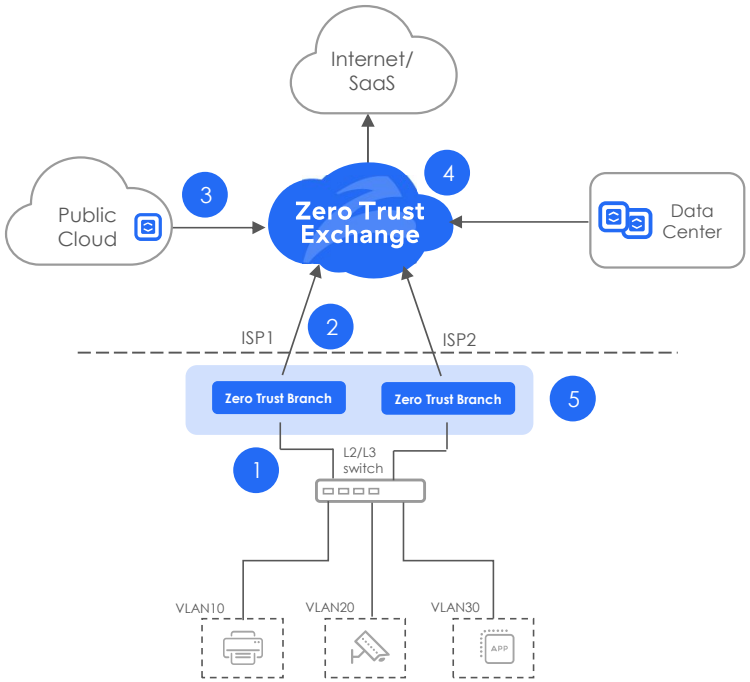
1. **Built-in DNS proxy/gateway responds with Synthetic IPs**
   Granular DNS policy control for local, remote and internet destinations

2. **Intercept and forward traffic to ZTE via outbound TLS connection**
   Destined to specific app, domains or synthetic IP range

3. **An outbound TLS connection from App Connectors**
   Existing ZPA App Connectors (no new deployment)

4. **Zscaler ZTE brokers the TLS connections based on the policy**
   Extends the granular ZPA access polices for Branch to App communications

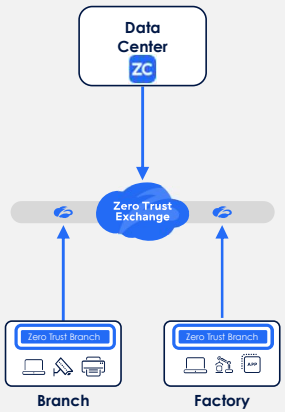
5. **Built-in App Connectors for inbound to Branch**
   App Connectors creates outbound connections to ZTE, eliminates inbound attack surface



Zero Trust Branch: Plug & play physical or virtual appliances

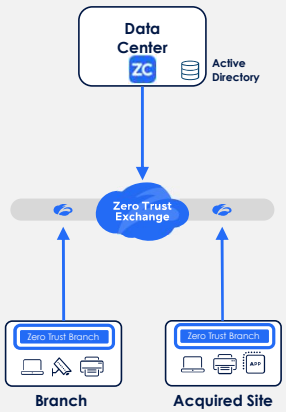
ZT Branch - SD-WAN Key Use Cases

Cafe-like Branches - ZIA



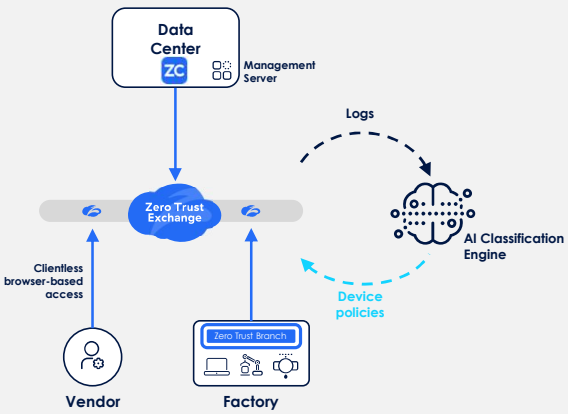
- No firewalls, VPNs or route tables to manage
- Eliminate intra-site movement and attack surface

Accelerate Agency Consolidation - ZPA



- Connect users to apps without merging routing domains
- Eliminate intra-organization movement and attack surface

Secure OT Environments - PRA



- Segment & Secure IT/OT environments
- Eliminate VPNs, jump hosts that provide vendor access to your network

Zscaler Zero Trust SD-WAN: Summary

Eliminates site-to-site VPNs

Zero trust network overlay connects users and devices to apps and prevents lateral movement

Extends zero trust beyond users

Enforce consistent security policies across users, IoT/OT devices, apps

Reduces complexity and cost

Simplified deployment, eliminates additional branch firewalls, route table management

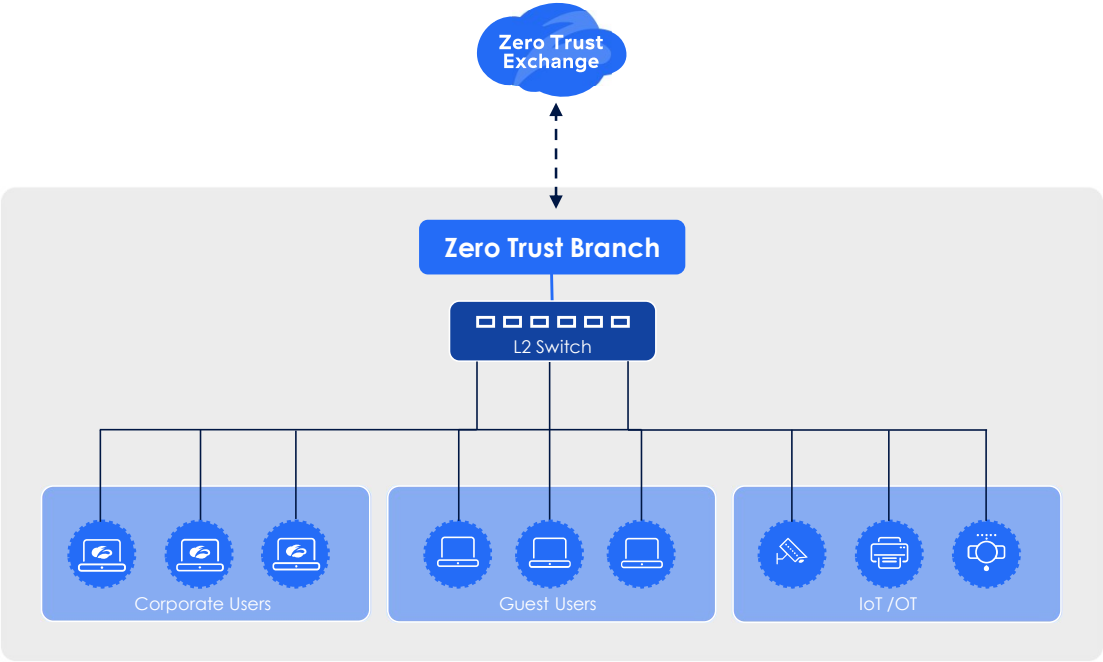
Pre-integrated with industry-leading SSE to deliver SASE powered by Zero Trust & AI

Zscaler Zero Trust Device Segmentation

Zscaler Zero Trust Device Segmentation

Agentless Segmentation for the Branch, Campus, Factories and Hospitals

- Isolate every device in the network without any endpoint agents
- Discover, profile & visualize all connected assets
- Adaptive policy engine with Kill Switch controls East-West traffic



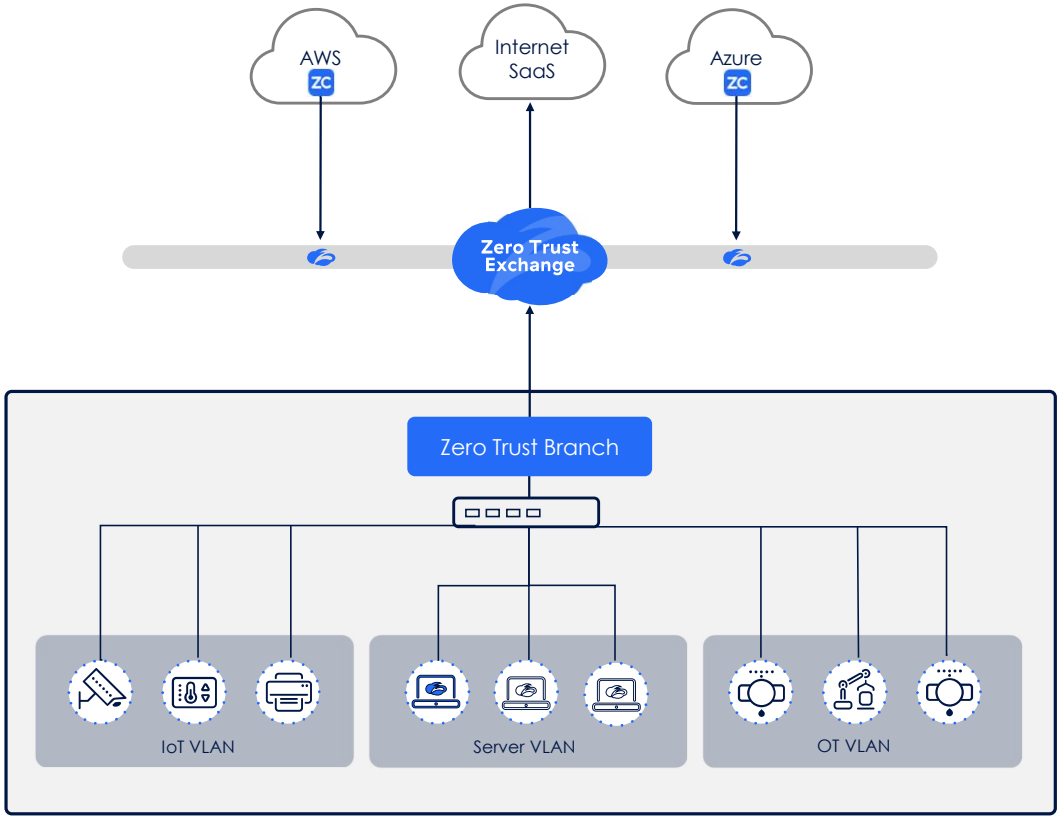
No attack surface

No lateral movement

No firewalls

How Zscaler Zero Trust Device Segmentation Works

Isolate every device in a "Network-of-ONE" without any agents or endpoint software

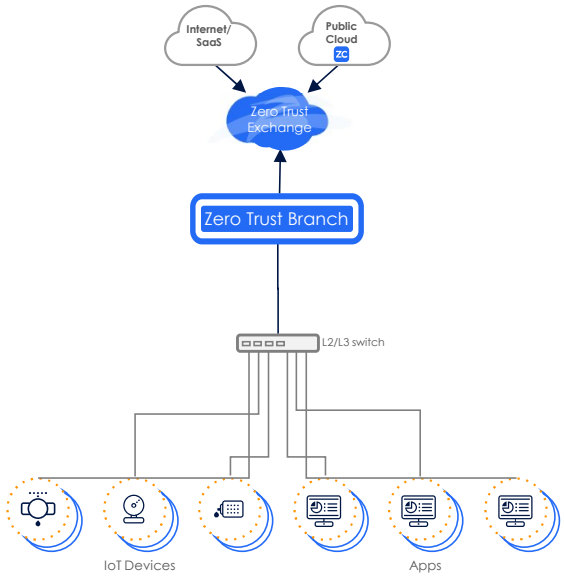


Zero Trust Branch, Campus, or Factory

1	Assumes the role of default gateway for VLANs
2	Auto-provisions every endpoint with a /32 subnet mask through the intelligent DHCP proxy
3	Automatically classifies device into groups (IT, IoT, OT, Servers)
4	Enforces group-based policies e.g. RDP access to cameras denied except from Admins
5	Ransomware Kill Switch™ enforces policies based on threat level for faster incident response

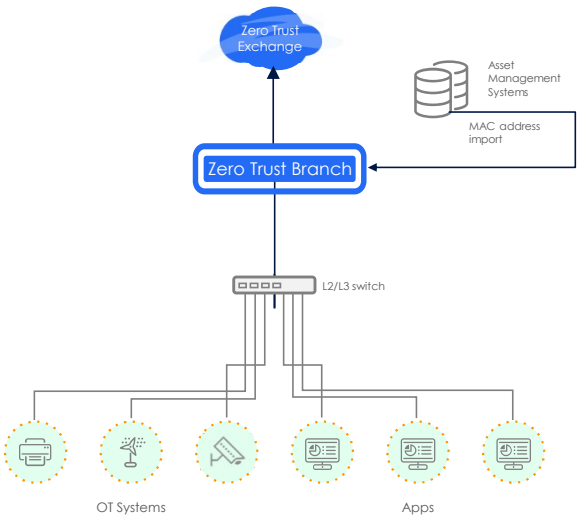
ZT Branch - Device Segmentation Key Use Cases

East-West Firewall Replacement



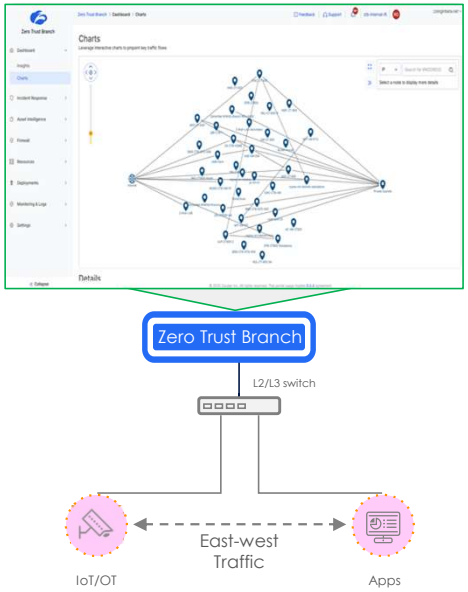
- Becomes the default gateway for VLANs
- Dynamic policy enforcement for all east-west traffic

IT/OT Segmentation



- Automatic isolation of unknown MAC addresses
- Asset Management System Integration – (Armis, Ordr)

Automatic Device Discovery & Classification



- Autonomous device discovery and classification
- Third Party SIEM Integration

Device Isolation Deep Dive

Key Concepts with "Network-of-ONE" subnet mask

Technology based on "first principles"

- Separation of routing (L3) and switching (L2) layers in TCP/IP
- Default gateway becomes next-hop for all other IP addresses
- Layer 3 to the endpoints eliminates direct communications over L2

Network-of-ONE Mask Assignment

- DHCP: As a DHCP Server or Relay adjusts option 1 (mask) in responses
- Remote PowerShell or GPO or Python scripts for well-known OSes
- Manual Change: Settings updates during service maintenance

Technology Adoption

- Early adopted by the telecom service providers
- Cloud service providers like e.g., Google Compute
- Point-to-Point tunnels (e.g., VPN, GRE etc.)

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : agndemo.com
   Link-local IPv6 Address . . . . . : fe80::8378:c7d3:ca28:d27b%14
   IPv4 Address. . . . . . . . . . . : 10.245.150.24
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 10.245.150.1
```

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     10.245.150.1    10.245.150.24     25
    10.245.150.24  255.255.255.255         On-link     10.245.150.24    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     10.245.150.24    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     10.245.150.24    281
===========================================================================
```

```
Interface: 10.245.150.24 --- 0xe
  Internet Address      Physical Address      Type
  10.245.150.1          0a-d3-4a-66-10-96     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

Zscaler Device Segmentation Benefits

Eliminate Lateral Threat Movement

Extend zero trust to customer's internal networks (LAN) without adding complexity

Reduce Operational Complexity and Cost

Reduce cost by eliminating east-west firewalls at the campus and branch

Gain Enhanced Visibility into East-West Traffic

Discover, classify and inventory devices without needing endpoint agents

Extend the power of the Zero Trust Exchange to your LAN

Zscaler Cellular Customer Use Cases

Vending Machines
Deliver all in one "secure service"

Point of Sales
Secure Payments

Machinery
Protect services & ensure integral access

ATM / Financial
Secure comms for distributed and isolated financials

Logistics
Secure access in and out of services

Rail Services
Protect services & ensure integral access

Charging
Ensure bidirectional control and security

Tablets / Kiosks
Provide agentless access to Internet & internal resources

Hand Scanners
Track packages and services

Critical Infrastructure
Ensure accurate Signals

Out of Band
Secure protection for support systems

Employee Management
Protect and Support time recording

Robotics
Secure access in and out of services

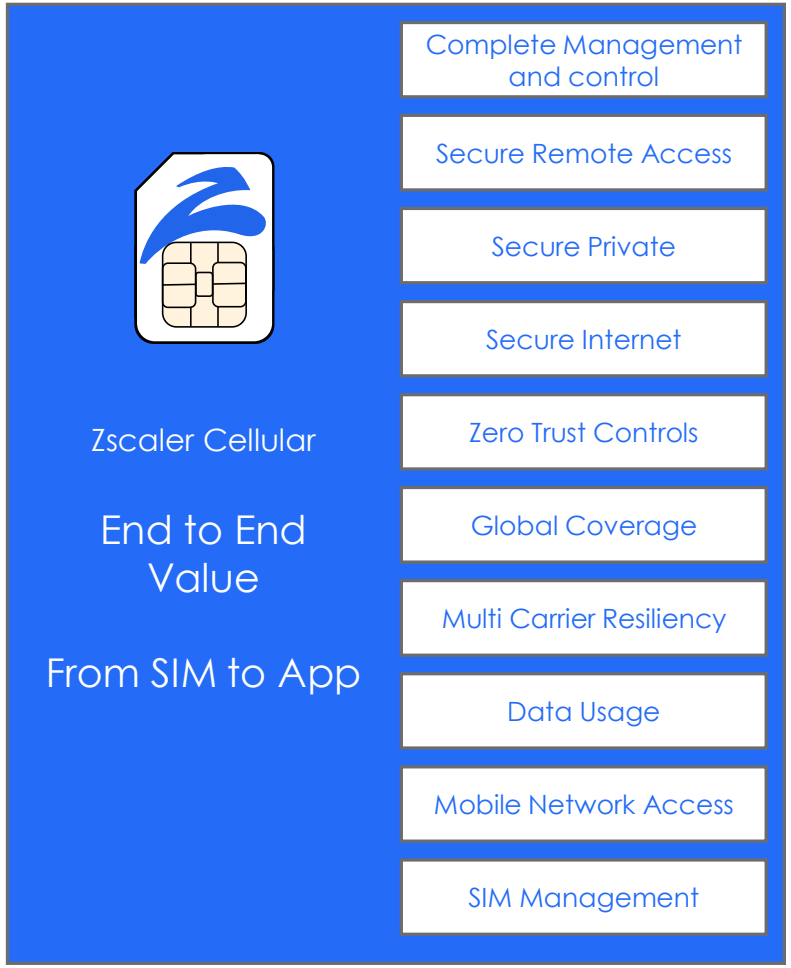
Military
Integral and protected comms

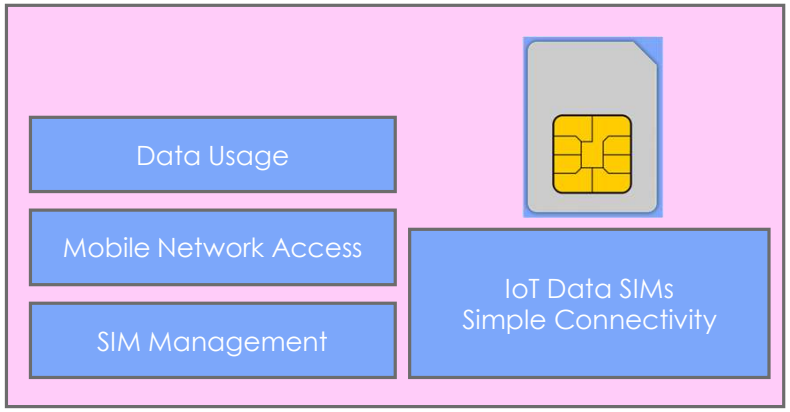
Automotive
Ensure secure comms

Secure GW
Protect downstream devices

A revolutionary way to secure and control every cellular-connected device across your enterprise.
We make your devices smarter, your networks impenetrable, and your complexity vanish.

Zscaler Cellular Value: Much More Than Connectivity





Resources

Resources

Zscaler Named a Leader in the 2025 Gartner® Magic Quadrant™ for Security Service Edge (SSE)
https://www.zscaler.com/blogs/company-news/zscaler-named-leader-2025-gartner-r-magic-quadrant-tm-security-service-edge-sse

Zscaler Named a Visionary in the 2025 Gartner® Magic Quadrant™ for SASE Platforms: Excited for the Zero Trust Branch
https://www.zscaler.com/blogs/product-insights/zscaler-named-visionary-2025-gartner-r-magic-quadrant-tm-sase-platforms

Zero Trust Branch
https://www.zscaler.com/products-and-solutions/zero-trust-branch

Zscaler Cellular
https://www.zscaler.com/products-and-solutions/zscaler-cellular

Thank You