Zscaler on Zscaler:

Reimagining Branch Security and Connectivity with Zero Trust Branch

WHITEPAPER

Introduction

At Zscaler, we have always believed that the future of enterprise connectivity lies in the cloud. But believing it and living it are two different things. For years, our own branch offices relied on fully redundant hardware stacks: dual Juniper firewalls and Arista WAN routers. This model was designed for an era when applications lived in the data center—but that era has long passed.

With the rise of SaaS, hybrid work, and the cloud-first enterprise, our infrastructure model had become not just outdated, but a friction point and a barrier to agility and growth. The challenge was clear: how could we lead from the front and prove to the world that Zscaler itself could move away from traditional firewalls and embrace the zero trust future?

Facing the Challenge

The decision to dismantle our traditional perimeter defenses was not one we took lightly. Firewalls had been the backbone of enterprise security for decades, and even within Zscaler, convincing our network and security engineers to trust the cloud over physical appliances was not easy. Some were skeptical that cloud-delivered security could match the scale, reliability, and robust protection offered by redundant firewalls. A key concern was how to secure IoT devices like espresso machines, water machines, and printers, especially in the absence of east-west firewalls. They worried that relying on a cloud security platform would introduce latency, negatively impacting the user experience compared to direct internet access.

We addressed these concerns through open communication, architecture reviews, and collaborative workshops that highlighted the risks and limitations of the legacy firewall model, alongside the significant benefits of a cloud-first approach.

What drove us was our commitment to living the values we share with customers: if we tell the world that the perimeter is gone and the future is zero trust, then we must prove it within our own enterprise.

The Transformation Journey

Over the course of four quarters, we embarked on one of the most significant infrastructure transformations in our company's history. Ten of our largest global sites were migrated away from firewall stacks and redundant WAN switches to Zscaler Zero Trust Branch (ZTB). Each deployment was designed to minimize disruption, and the results exceeded our expectations: migrations were completed in hours instead of days. What once required weeks of hardware procurement, shipping, and complex cutovers is now a simple, plug-and-play process that connects branches directly to the Zscaler Zero Trust Exchange platform.

Following the migration, all user traffic—employees, guests, and IoT—now flows through the Zero Trust Exchange. Internet traffic is inspected inline for threats, all SaaS services are accessed securely through Zscaler Internet Access (ZIA), and any connection to private resources is brokered through Zscaler Private Access (ZPA). This ensures that every user, in every location, receives the same consistent security and optimized experience.

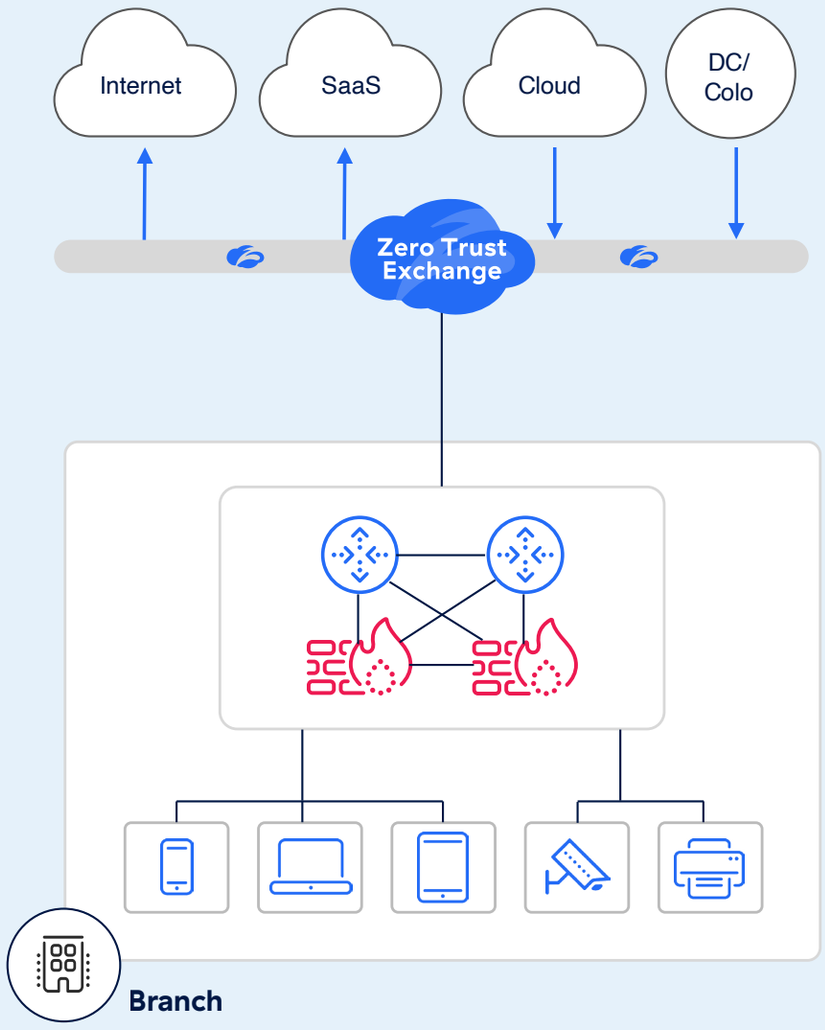


Figure 1: Prior architecture relied on legacy on premise firewalls

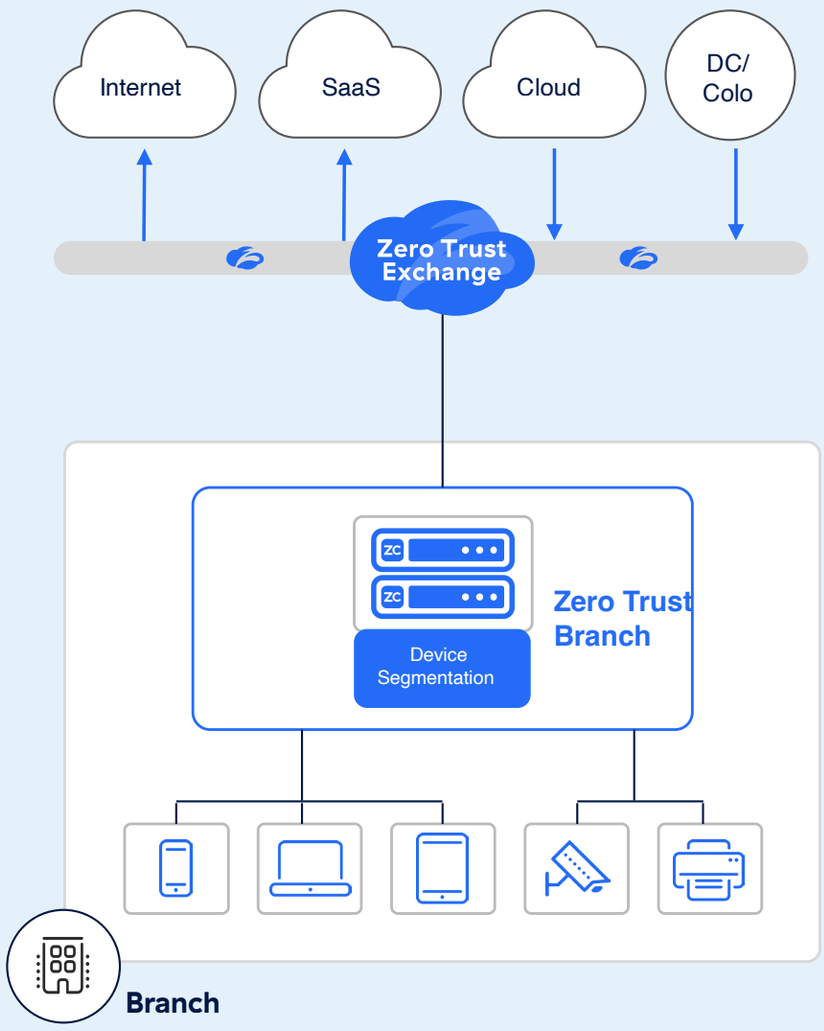


Figure 2: New architecture provides Café like simplicity, improved security, and lower cost

Transformation Timeline

Our journey was not a single step but a carefully structured evolution:

Preparation and Alignment: Q1 FY25

We began by building consensus across our internal network and security engineering teams. This included multiple architecture reviews, technical deep dives, and open forums where skeptics could voice concerns. The groundwork was critical: aligning on a vision and addressing fears before the first cutover.

Pilot and First Migrations: Q2 FY25

With alignment achieved, we launched pilot migrations at select sites. These early successes proved that Zero Trust Branch cutovers could be executed in hours, not days, with minimal disruption. The pilots served as both validation and a cultural turning point. Cloud-delivered firewalling and URL filtering caused no noticeable delays or negative impact on user experience. Furthermore, agentless zero trust segmentation was successfully implemented across IoT and OT devices, encountering no interoperability or application challenges. This proved that east-west firewalls were a thing of the past.

Global Rollout: Q3 and Q4 FY25

Armed with lessons learned, we accelerated the program. Ten of our largest global offices were transformed, legacy firewalls and WAN hardware were decommissioned, and staff shifted their focus from maintaining appliances to enabling strategy.

Post-Migration Reality

Today, every branch operates on the same secure foundation. All branch traffic flows through the Zero Trust Exchange, SaaS and general internet are accessed directly via ZIA, and private applications are connected seamlessly through ZPA. Branch offices and remote workers now benefit from a cohesive, cloud-delivered security framework, replacing the previous assortment of hardware and disparate policies.

Preparation and Alignment	Pilot and First Migrations	Global Rollout	Post-Migration Reality
Q1 FY25 (Aug - Oct 2024)	Q2 FY25 (Nov 2024 - Jan 2025)	Q3/Q4 FY25 (Feb - July 2025)	Today

Technical and Strategic Foundations

The strength of this transformation lies not just in execution, but also in the architectural principles that guided it. The Zscaler Zero Trust Branch reference architecture provided the framework that made this scale of change possible.

- **Zero trust, not network trust:** Access is enforced at the application level rather than the network level, eliminating lateral movement and shrinking the attack surface.
- **Zero touch provisioning:** Branch devices were shipped, plugged in, and automatically configured via the Zscaler cloud. Global deployment became swift, straightforward, and low-risk. By utilizing third-party Smart Hands, we also eliminated expensive travel to each location.
- **Flexible deployment modes:** Smaller sites adopted Gateway Mode (providing NAT, DHCP, VLAN support, and load balancing), while larger campuses used One-Arm Mode to integrate seamlessly with existing infrastructure.
- **High availability by design:** Each branch gained resilience through hardware-level redundancy and continuous cloud-level monitoring with WAN link failover, ensuring no downtime even as legacy firewalls were removed.

- **Policy-based forwarding:** Traffic is routed intelligently—sent to ZIA for internet, ZPA for private apps, or securely blocked if unauthorized—enforcing least-privileged access globally.

- **IoT/OT microsegmentation and integration:** Built-in AppConnector capabilities provided secure, clientless access (SSH, RDP, VNC) for IoT/OT devices, while profiling and segmentation extended zero trust to non-user endpoints. By segmenting IoT/OT devices into individual /32 segments, lateral movement on the Layer 2/3 network is eliminated.

- **Unified management console:** All policies, monitoring, and analytics are enforced centrally, giving operations full visibility and eliminating the inconsistencies of site-by-site firewall rules.

Following these design principles, we achieved both a technical and strategic win: we eliminated complexity, strengthened security, and gave our IT and security leaders a model that scales with the business.

The Uniqueness of Zscaler on Zscaler

Zscaler runs on Zscaler—we are Customer Zero. This is the most unique aspect of our journey. Unlike many vendors, we put our own products at the core of our global operations, creating both a unique opportunity and a unique challenge.

On one hand, it means we validate our own solutions at enterprise scale every day. Our engineers, employees, and business units all experience firsthand the security, agility, and user experience that we promise our customers. This transparency strengthens trust when we engage with CIOs and CISOs—we are not only advocates, but proven practitioners.

We hold ourselves to the highest standards, understanding there's no room for error when our company operates on the same platform we offer customers. This commitment thoroughly tested the Zscaler platform's capabilities as we convinced skeptical engineers, addressed their concerns, and designed a resilient architecture for our global operations. Our Zscaler on Zscaler team, by using our products in a production environment, identified 19 software bugs and submitted 10 enhancement requests, finding issues and validating resolutions with our product teams. In every sense, we were "drinking our own champagne."

This duality—operating as both customer and provider—creates a feedback loop that continually improves our products. It ensures we uncover and solve challenges early, before our customers face them, and it allows us to demonstrate leadership by example.

Security and Networking Benefits

Our security posture underwent a fundamental change. All corporate-owned devices in every office now benefit from inline threat prevention, DLP, CASB, and full SSL inspection at scale. Guest and IoT traffic are now also routed to the Zero Trust Exchange, benefiting from inline threat prevention.

Seamless segmentation eliminates exposed attack surfaces and reliance on implicit trust. Our networking teams gained agility by removing the need for complex WAN hardware, shifting instead to simple, direct-to-cloud connectivity via broadband and 5G, optimized by Zscaler's 160+ global data centers. The operational burden of patching and maintaining physical firewalls disappeared instantly.

Business Impact

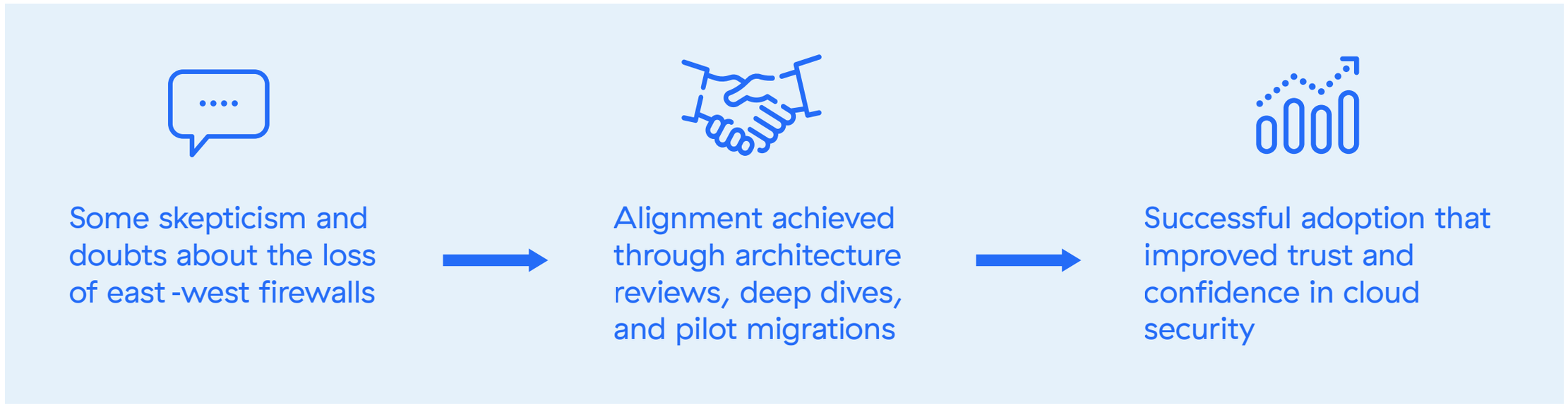
The transition to an as-a-service model for hardware immediately eliminated capital costs entirely, removing the need to purchase and refresh expensive firewall and WAN hardware. This shift delivered transformative financial and operational benefits. Furthermore, ongoing support and maintenance expenses were reduced by 30%—43%, depending on the office size. Staff were freed from the endless cycle of managing on-premises appliances and could focus on higher-value, strategic initiatives. Most importantly, the business gained agility: new offices could be brought online in hours, not weeks, and employees experienced a faster, more reliable connection to SaaS, internet, and private applications. The migration proved that a simpler infrastructure can deliver stronger security, higher productivity, and lower costs.

Business Outcomes	Security Outcomes
Improved Business Agility	Reduced internal attack surface
Enhanced End User Experience	Securely harnessing Gen AI with DLP
Cost Reduction	Ecosystem precision and speed
Simplicity	Proactive defense

User Experience and Cultural Shift

One of the most profound outcomes of this journey has been the user experience. Employees no longer worry about VPNs or slow connections caused by backhauling traffic. Whether at headquarters, in a branch, or working remotely, the experience is seamless, secure, and consistently fast. What once felt like friction has been replaced by confidence and speed.

Culturally, this transformation was also a turning point for our internal teams. Through countless meetings, architecture reviews, and frank discussions, we aligned on a shared vision. We demonstrated to even the most skeptical engineers that zero trust everywhere is not just a theory—it is a better way to run enterprise infrastructure. That cultural shift was just as important as the technical cutovers, because it proved that trust in the cloud can replace trust in the perimeter.



Conclusion

The Zscaler on Zscaler initiative is more than an internal IT project—it is a statement of leadership. By replacing traditional firewalls and WAN routers with Zero Trust Branch, we showed the world that Zscaler practices what it preaches. We proved that even the most critical sites can be migrated in hours with zero outages, delivering superior security, improved performance, and lower costs.

Our journey was not without challenges, but it reinforced our conviction that the future of branch connectivity is not more hardware. It is less hardware, more cloud intelligence, and a zero trust approach that enables agility, security, and innovation. For CIOs and CISOs, the lesson is clear: this is not just a technical upgrade, but a strategic shift that unlocks business value and resilience. The perimeter is gone. Now is the time to adopt zero trust to secure operations and drive organizational agility.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

Zero Trust Everywhere