Enterprise connectivity challenges with legacy WAN connectivity

Hybrid work and cloud transformation have upended perimeter-based network and security models, with private applications moving to the cloud and users accessing applications over the public internet, on any device, from any location. Traditional approaches have become ineffective in the cloud- and mobile-first world.

Traditional WANs utilize SLA-backed private multiprotocol label switching (MPLS) or leased lines to an organization’s main data centers for application and security needs. But these come at a premium price. Many have switched to SD-WAN with IPSec (P2P) tunnels for connectivity. SD-WAN uses commodity links, such as broadband internet, LTE, etc., and allows you to intelligently manage and control connectivity between branches and cloud instances.

But with its benefits, SD-WAN also brings many challenges, such as a lack of security through network-based access, an increased attack surface, extensive privileges, and routing complexity. These existing solutions still connect networks using VPNs, which do not adhere to zero trust principles. Zscaler provides Zero Trust Branch Connectivity for users, servers, and IoT/OT devices in branches for secure connectivity and simplified operations without routing complexities or a degraded user experience.
Zscaler Zero Trust Branch Connectivity replaces traditional WANs

Zscaler Zero Trust Branch Connectivity replaces traditional WAN connectivity solutions in the branch by bringing zero trust principles to every connectivity need—not just for users, but also for servers and IoT/OT devices. The Zscaler Zero Trust Exchange direct-to-cloud architecture eliminates the attack surface and lateral threat movement with a non-routable WAN network. Zscaler helps you modernize branch and data center connectivity with quicker SaaS and cloud app deployments, local internet breakouts, and eliminates site-to-site VPNs. With integrated and automated connectivity and security, it reduces complexity and cost and provides a faster, smarter, and more secure alternative to legacy network solutions.

Zero Trust Branch Connectivity use cases

Direct internet access enablement for branches
On-premises networking and security models become less effective as organizations migrate their apps to the cloud and build cloud native apps. Zscaler Zero Trust Branch Connectivity is a purpose-built solution for branch transformation, ushering in a new model where branches communicate with any destination securely and independently from the underlying network.

Site-to-site VPN replacement
Connect branches directly to private applications without extending your WAN or relying on VPNs, both of which increase a network’s attack surface. Applications are hidden from discovery behind the branches, and access is restricted via the Zscaler Zero Trust Exchange to a set of named entities. Identity, context, and policy adherence of the specified participants are all verified before access is allowed, prohibiting lateral movement elsewhere in the network.

Shadow IoT/OT discovery and visibility
IT teams face blindspots as unsanctioned, undiscoverable devices connect to branch office networks, and the result is an increase in device vulnerability and a broader attack surface. Zscaler identifies and classifies devices to give IT teams deeper visibility into behavior for better access control policies.

Zero trust for server, IoT/OT connectivity
IoT/OT assets need to be regularly accessed by employees and third-party vendors to maximize production uptime and avoid disruptions from equipment and process failures. Zero Trust Branch Connectivity for IoT provides fully isolated, clientless remote desktop access to internal RDP and SSH target systems—without having to install a client on their device using jump hosts and legacy VPNs.
Mergers and acquisitions

Merging two separate networks is challenging and time-consuming. Problems range from IP overlaps to routing issues to increased security risk from an enlarged network attack surface. With Zscaler Zero Trust Branch Connectivity, networks can remain separate and branch locations in one environment can quickly connect to private applications in another without disruption.

Core Capabilities

- **Cost effective branch and data center connectivity**
  Eliminate the need to provision and manage VPN/MPLS connections between the branch and the data center. Instead, establish inside-out DTLS connections across on-premises and hybrid clouds, brokered through the Zero Trust Exchange.

- **Zero touch provisioning and automated deployment**
  Zscaler Zero Trust Branch Connectivity allows zero-touch deployment and automated policy configuration across branches and data centers. It can also be auto-deployed across multiple branches within minutes.

- **Secure ingress and egress control**
  Zscaler Zero Trust Branch Connectivity takes an allowlist approach and enables granular ingress and egress controls for branches communicating with internet services. In addition, centralized policy management enforces consistent and standardized security policies across branch, multi-cloud and data center environments.

- **Complete visibility and reporting**
  Zscaler Zero Trust Branch Connectivity provides granular audit-compliant logging of all forwarded application traffic and its associated access information. In addition, it supports Nanolog Streaming Service (NSS) to stream all logs to customer’s SIEM in real-time automatically.

- **Part of the world’s largest security cloud**
  Zscaler Cloud Connector leverages the proven scale, performance, and reliability of the Zero Trust Exchange to ensure safe, controlled access from any cloud, with no exposed attack surface.