Zscaler Zero Trust Branch Connectivity

Enable zero trust connectivity in branches and data centers from any user, server, and IoT/OT device in any location, over any network.

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 that rely on legacy WAN, mesh VPNs, and firewalls to control application access have become ineffective in a cloud- and mobile-first world.

Traditional WANs utilize SLA-backed private multiprotocol label switching (MPLS) or leased line links to an organization’s main data centers for all application and security needs. But these come at a premium price. Many businesses have switched to an alternative transport architecture SD-WAN and 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.

Though there are many benefits to be had, SD-WAN also brings challenges, such as a lack of security through network-based access, a broad attack surface, extensive privileges, and routing complexity. All 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:

• Enables zero trust everywhere for all users, devices, servers, and IoT/OT regardless of location, shifting implicit access to explicit access per application based on continuous identity and context validation.

• Securely connects all offices to every data center, multicloud, and SaaS by building a foundation for secure connectivity that enables east–west segmentation to prevent lateral threat movement while delivering superior user experiences.

• Eliminates the attack surface as branches and data centers are connected directly to each other through Zscaler Zero Trust Exchange independent of their underlying corporate network, VPN, or WAN.

• Sits on a purpose-built, multitenant proxy architecture that holds, inspects, and enforces policy.

• Delivers high–performance inspection done by a single scan multi–action (SSMA) architecture that’s built for scale.

• Enforces finely–grained forwarding policies for internet and non–internet traffic using Zscaler Internet Access or Zscaler Private Access.

• Unifies and standardizes policies across branches, data centers, and multicloud locations. This includes policy management, traffic monitoring, and log tracking.

• Identifies and classifies devices for deeper visibility into behavior for better access control policies.
Enterprise connectivity challenges with legacy WAN connectivity

Organizations face several challenges when using a legacy network and security architecture to connect a branch to the internet or to their other applications in a public cloud or data center environment, including:

- **Greater risk of lateral threats and internet-based attacks** from using legacy, network-centric connectivity solutions such as site-to-site VPNs, firewalls, or WAN technologies. These solutions overextend a customer’s trusted network across the internet to other clouds and on-premises environments, increasing the attack surface. A patchwork of security appliances, tools, and non-standard policies lead to increased security risk due to known and unknown gaps in security coverage.

- **Increased complexity** due to complicated routing, multiple network hops and appliances, and fragmented policy management from introducing legacy models to the cloud. Managing this complexity is a difficult task for networking and security teams as they struggle to standardize connectivity and enforce security policy across branch, cloud, and data centers.

- **Lack of visibility** across branch, data center, and cloud connectivity paths, which creates network and security blind spots.

![Diagram showing network connectivity options](image)

**Internet/SaaS**

- **Local Internet Breakouts**
- **Direct Connect/Express Route**
- **SD-WAN over the internet replaces MPLS** Site-to-site VPNs extend the network to branches, factories, IaaS/PaaS, and more
• **Poor performance and scalability** due to the increasing number of network and security services within branch and data center environments, traffic hairpinning, and chokepoints for centralized security inspection and control.

• **High costs** due to legacy network and security appliances (e.g., firewalls, IPS, routers, and other point products), overprovisioning of network services to compensate for lack of scalability, and increased use of cloud native services.

---

**Zscaler Zero Trust Branch Connectivity replaces traditional WAN connectivity**

Zscaler Zero Trust Branch Connectivity replaces traditional WAN connectivity solutions in-branch by applying zero trust principles to user, server, and IoT/OT device connectivity. The Zscaler Zero Trust Exchange’s direct-to-cloud architecture eliminates the attack surface and lateral threat movement with a non-routable WAN network.

In the past, managing a limited number of locations using standard connectivity and security architectures was doable. Businesses would typically try to connect these locations using WAN, a mesh of VPNs, MPLS, or ‘automated solutions’ with SD-WAN and IPSec (P2P) tunnels for connectivity. All these existing solutions still connect networks using VPNs, which cannot do zero trust.

Zscaler Zero Trust Branch Connectivity provides branches and data centers fast and reliable access to the internet and private applications with a direct-to-cloud architecture, which provides high security and operational simplicity. It eliminates the network attack surface by establishing direct branch-to-internet and branch-to-private app connections using a full proxy architecture. What’s more, it dramatically simplifies branch communications by eliminating complex routing, VPNs, firewalls, while allowing for flexible forwarding and simple policy management by using the proven ZIA and ZPA policy framework.

All branch communications are forwarded directly to the Zero Trust Exchange, where ZIA or ZPA policies can be applied for full security inspection and access identity-based control of branch and data center communications. The communications are then forwarded from the Zero Trust Exchange to any destination, whether it be the internet or other private applications in a public cloud or an on-premises data center. This unique approach provides three key advantages:

• You move away from network-based site-to-site VPN connectivity to identity and application-based communication for true, zero trust security

• You eliminate a legacy castle-and-moat architecture without compromising security; no need for legacy products such as Squid proxies, NAT gateways, IPSs and so on

• You provide distributed, scalable connectivity wherever it’s needed, with centralized, automated policy management to simplify branch and data center communications
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/OT 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.

<table>
<thead>
<tr>
<th>TABLE 1: ZSCALER ZERO TRUST BRANCH CONNECTIVITY CAPABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE</strong></td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
</tr>
</tbody>
</table>
| Zero touch provisioning and automated deployment | • Zero touch provisioning with pre-defined templates  
• Fully automated deployment  
• Dynamic discovery of branch office geo-location  
• Built-in SLA monitoring and failover |
| Granular forwarding policy for internet and private application traffic | • Options to send the traffic to ZIA, ZPA, or Direct (bypassing Zscaler services)  
• Flexible traffic selection criteria location, sublocation, location group, 5 tuple, or FQDN  
• Built-in availability with seamless failover to next available service PoP |
| Unified zero trust policies | • Dynamic locations for branch and data center, such as existing ZIA locations, are synchronized with the ZIA platform  
• Security policy enablement that includes IPS, SSL proxy, URL filtering, and data protection  
• A full security stack with posture configured on ZIA for servers and IoT/OT  
• Unified policy for user-to-application, IoT device-to-application, and server-to-server through ZPA’s enhanced policy to include new client types |
| High availability | • Automatic failover with N+2 redundancy ensures service continuity  
• Two instances of Branch Connector provide additional support for traffic bursts and redundancy in case of a hardware failure  
• A load balancer is configured for active-passive fault tolerance using a virtual IP address (VIP) using common address redundancy protocol (CARP) |
| Centralized visibility and granular logging | • Centralized dashboard for device health and traffic monitoring  
• Available filtering for cloud, data center, and branch deployments  
• Detailed logging of every session and transaction for all ports and protocols—including all public and private DNS transactions  
• Full integration with NSS infrastructure—existing NSS firewall VM can be used to stream the logs to SIEM |