Zscaler Zero Trust Branch Connectivity

Enable zero trust connectivity in branches and data centers from any user, server, or 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.

In today’s landscape, many enterprises also leverage IoT/OT devices across various locations—including branches, factories, and data centers—to streamline their business operations. Additionally, a considerable number of customers rely on server-to-client workload communication to fulfill their business needs. Traditional approaches that depend on legacy WANs, mesh VPNs, and firewalls to manage application access have become ineffective in a world that prioritizes cloud and mobile technologies.

However, as business requirements have evolved, legacy WAN solutions struggle to keep pace. SD-WAN presents various challenges, such as limited security through network-based access, an expansive attack surface, extensive lateral movement privileges, and routing complexities. Layering on zero trust principles to this network often requires adding additional firewall appliances, adding cost and complexity.

Zscaler Zero Trust Branch Connectivity:

- Enables zero trust everywhere for all users, devices, servers, and IoT/OT, regardless of location
- Improves application performance by sending traffic directly to the Zero Trust Exchange
- Prevents lateral threat movement: zero trust builds a foundation for secure connectivity that enables east–west segmentation
- Eliminates the attack surface by connecting branches and data centers through Zero Trust Exchange independent of the underlying transport
- Enables shadow IoT device discovery and classification with automatic device classification based on traffic profiles
- Simplifies secure access to OT resources with clientless browser-based access to SSH/RDP/VNC ports on OT assets
- Enforces finely-grained forwarding policies for internet and non-internet traffic using ZIA or ZPA
- Introduces plug-and-play deployment: zero touch provisioning (ZTP) simplifies deployment and reduces time to integration

© 2023 Zscaler, Inc. All rights reserved.
Zero Trust Branch Connectivity securely connects your branches, factories, and data centers without the complexity of VPNs, ensuring zero trust access between users, IoT/OT devices, and applications based on business policies.

**Challenges with legacy WAN technologies**

Organizations face several challenges when using legacy network and security architectures 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.

• **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.

Figure 2: Greater risk of lateral threats and internet-based attacks with legacy WAN solutions
How Zero Trust Branch Connectivity works

Zero Trust Branch Connectivity dramatically simplifies branch communications by eliminating complex routing, VPNs, and 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 provide distributed, scalable connectivity wherever it’s needed, with centralized, automated policy management to simplify branch and data center communications
- 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

Zero Trust Branch Connectivity use cases

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 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.

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

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 that enables branches to communicate with any destination securely and independently from the underlying network.

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 RDP and SSH target systems—without having to install a client on their device using jump hosts and legacy VPNs.

**Shadow IoT/OT discovery and visibility**

IT teams face blind spots 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.

### Branch Connector Hardware and Software Models

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>ZT 400</th>
<th>ZT 600</th>
<th>ZT 800</th>
<th>ZT VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Small–Medium branches</td>
<td>Small–Medium branch</td>
<td>Medium–Large branch</td>
<td>Branch and Data Center</td>
</tr>
<tr>
<td>Throughput/hypervisor</td>
<td>200 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>KVM, ESXi</td>
</tr>
<tr>
<td>Physical ports</td>
<td>4 x GbE</td>
<td>6 x GbE</td>
<td>8 x GbE</td>
<td>N/A</td>
</tr>
<tr>
<td>Zero touch provisioning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Granular forwarding policy for internet, private applications, and direct WAN traffic</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Leverage URL filtering, file type control &amp; cloud firewall policies for internet bound traffic</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Zero Trust ZPA policies for IoT devices, servers</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Centralized visibility and logging</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FEATURE</td>
<td>DETAILS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></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 |