Deploying Zscaler Internet Access™ in China

Reference Architecture

Contents

About Zscaler Reference Architectures Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who is this guide for?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A note for Federal Cloud customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler account team on feature availability and configuration requirements.

Conventions used in this guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding out more

You can find our guides on the **Zscaler website** (**https://www.zscaler.com/resources/reference-architectures**).

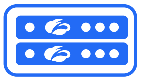
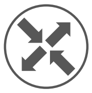
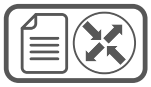
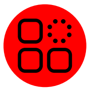
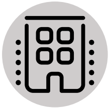
You can join our user and partner community and get answers to your questions in the **Zenith Community** (**https://community.zscaler.com**).

Terms and acronyms used in this guide

Acronym	Definition
CPE	Customer Premises Equipment
DC	Data Center
DMZ	Demilitarized Zone
GFW	Great Firewall
GRE	Generic Routing Encapsulation
IPSec	Internet Protocol Security
PAC	Proxy Auto-Config file
PoP	Points-Of-Presence
SD-WAN	Software-Defined Wide Area Network
SSL	Secure Socket Layer (superseded by TLS)
TLS	Transport Layer Security
WAN	Wide Area Network
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

Icons used in this guide

The following icons are used in the diagrams contained in this guide.

ZIA Service Edge	
Zscaler Cloud Router	
Zscaler Client Connector on Devices	
Router	
SD-WAN Device	
Application inside China	
Application outside China	
Branch Office	

Introduction

Accessing the internet from China is a well-known issue for many organizations. Where in most of the world you can expect consistent and unregulated access, China is unique in its complexity as both the technical and regulatory environments change rapidly.

To understand the complexities involved, it helps to have some background on China's internet access. The Great Firewall (GFW), a content filter where the internet is heavy regulated and always monitored, exists between China and the rest of the world. China has three tier 1 providers: China Unicom in the north, China Telecom in the south, and China Mobile providing cellular access.

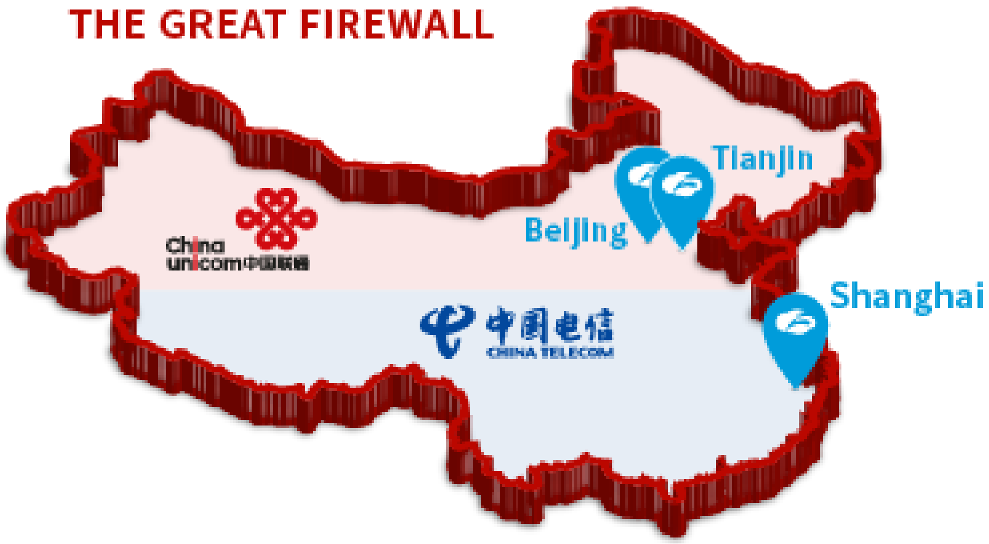


Figure 1. China has two primary ISPs, each with ZIA Public Service Edge deployments

Internet access from within China, both to services within the country and across the international link, can be expensive and congested. Premium links that have much higher bandwidth available can be purchased, but at a high cost per megabit. The common international link tends to be highly congested during business hours. Generally, access between carriers works, but each provider may also have differentiated policies and support.

Your organization must also be prepared to deal with inconsistencies in access resources from one day to the next. Regulatory changes happen regularly, such as being tighter during major political events within the country. Common web ports are blocked, preventing their use without a license. In other cases, code injections and network resets have been used to prevent application use.

To successfully operate within this environment requires a new approach to network operations. To help you navigate this difficult environment, Zscaler has developed solutions with service providers inside of China. Zscaler's partnership includes deploying ZIA Public Service Edge data centers within China, and ZIA Private Service Edge devices within the service providers themselves.

This guide discusses deployment options for ZIA use within China. We start out covering the operating environment in more detail, and then discuss your organization's options that include Zscaler China Premium Access with partners. ZIA premium access in China delivers many advantages including:

- Improved user experience – Increase productivity and deliver a better user experience for employees accessing international websites and SaaS applications, such as Microsoft 365, Salesforce, and ServiceNow.
- Reduced costs – Minimize operating expenses by eliminating on-premises equipment and delivering security and premium internet connectivity as a combined service.
- Simplified IT and reduced risk – Reduce deployment complexity, simplify IT, and reduce compliance risk by streamlining the delivery of security and internet connectivity.

We also discuss using a ZIA Public Service Edge, ZIA Private Service Edge, or ZIA Virtual Service Edge.

Zscaler's legal and regulatory status in China

Zscaler must operate within the laws and regulations of its host country. Zscaler is an overlay network and does not produce or serve its own content. A content request is generated by the end user, and the content provider delivers the response. If Zscaler did not exist, the request, response, and content delivery would still occur.

In China, only a content provider who is serving content from mainland China is required to have an ICP license. Zscaler does not generate or serve content in mainland China or offer additional encryption services.

Zscaler uses standard carrier connectivity to exit China and any Great Firewall. Zscaler does not have the ability to influence the enforcement of any restrictions. Our customers are contractually responsible for complying with all local regulatory restrictions when using our services and products.

Zscaler is constantly reviewing the dynamic regulatory landscape in China and reserves the right to take any measures necessary to ensure the security of all customers on its cloud, including but not limited to a suspension or shutdown of service.

As with any jurisdiction, it is the ultimate responsibility of our customers to ensure their compliance with local regulations when using Zscaler services.

The solutions presented in this guide represent Zscaler's best understanding of the operating environment in China at the time of publication. Zscaler strongly recommends you work with local representatives, both technical and legal, as you prepare for your deployment to understand what is possible.

New to leveraging ZIA in China or the Chinese market in general?

The following links provide resources to get you started understanding the complexity of deployments in China:

- Watch our webinar on **Transforming User Experience and Productivity for Your Employees in China** (**https://info.zscaler.com/webinar-transforming-user-experience-and-productivity-for-your-employees-in-china**).
- Watch a technical breakout from our **Zenith Live event** (**https://community.zscaler.com/t/deploying-the-zscaler-zero-trust-exchange-in-china/12754**).
- Read about China's Personal Information Protection Law ("PIPL") and **Zscaler's compliance** (**https://www.zscaler.com/privacy-compliance/pipl**).
- Read the technical setup details on our **help site** (**https://help.zscaler.com/zia/china-premium-internet-access**).
- Read our blog **How to Solve the Challenge of Connectivity in China** (**https://www.zscaler.com/blogs/product-insights/how-solve-challenge-connectivity-china**).

Understanding internet connectivity in China

Accessing the internet in China requires rethinking your standard approaches to internet access. Everything from speeds, costs, and support SLAs are different. This section discusses the environment that exists today. By understanding this environment and your organizational needs, you'll be able to select from the various access use cases presented later in the guide that best meet your organization's needs.

Zscaler's position in China

Most of the world is aware that China has one of the most regulated internet access policies in the world. When operating in China, both Zscaler and its customer have compliance responsibilities. The following summary is Zscaler's position while operating within China:

- Zscaler must operate within the laws and regulations of its host country, including China.
- Zscaler is an overlay network, not a VPN or content provider.
- Zscaler does not originate requests or create content.
- Zscaler cannot help you bypass content restrictions.
- Compliance and enforcement are the responsibility of the organization and end user.
- You should always consult regulatory requirements and in-country advisors to ensure that your network configuration complies.
- Zscaler recommends that you consult your local legal advisers before implementing any solution.

Zscaler strongly recommends that you work with local representatives and partners to understand the regulatory environment and your responsibilities. All changes to your network connectivity are made in conjunction with your ISP.

Policy enforcement in China

Internet connectivity in mainland China is strictly regulated by the Chinese government. The laws include banning various types of content and sites, and ongoing traffic inspection. Polices have gotten stricter over time, and are further increased during politically sensitive times of the year. The availability of applications is also inconsistent; what may work one day can fail the next.

Policies are enforced by the GFW, which controls access. The ranges of actions that the collective enforcement technology can include are as follows:

- Blocking of URLs and IP addresses for domains such as Google or Facebook.
- Alteration and poisoning of DNS responses.
- Which applications are being used.
- Blocking based on keywords in the data.
- Injected TCP resets.
- JavaScript injections that interfere with application behavior.
- Other variables can also be blocked including ports and protocols.
- Other parameters and enforcement mechanisms that are not publicly disclosed.

The policies are subject to change without notice. At any given moment, certain types of traffic or destinations can either be blocked entirely or discouraged by throttling bandwidth. You may recover access or be permanently blocked.

We have observed that major events like elections, national or religious holidays, and political events within China correlate with an increase in erratic behavior. This includes application performance and availability degrading. Typically, this behavior begins shortly before the event itself, through the course of the event, and ends shortly after the event has passed.

Although Hong Kong and Macau are part of China, they are currently largely exempt from these regulations being outside the control of the GFW.

Internet connectivity in China

Within China there are two ground-based tier 1 ISPs: China Unicom in the north, and China Telecom in the south. The ISPs operate independently of one another and transiting between them generally works. Even within the same ISP, different regions have different rates and service offerings.

These providers also offer premium connections internationally. These links offer much more standard performance but at a high cost. These links can cost your organization hundreds of dollars per megabit per month, but this is the only solution for reliable access at this time.

In addition to the ISPs, there are also overlay networks, that help work around the inter-ISP complexities. These overlay networks provide consolidated network services, eliminating the end user complexity.

There are also cloud computing vendors that operate within China. These can provide additional hosting and gateway options, as well as private backbone access between their data centers.

Observations regarding traffic from China to international destinations

While providing services in China, Zscaler has had the opportunity to observe disruptive network behaviors while transiting the GFW toward international destinations. Having data centers on each side of the GFW allows us to gain insights into where issues are occurring.

These disruptions affect traffic originating in mainland China towards international destinations and occur most often during business hours. These network conditions affect all traffic in and out of China. This applies both to customers connecting to Zscaler DCs inside, and outside of China connecting to international destinations.

Certain ports, protocols (IPsec, GRE), or IPs are unreachable

Certain international destinations become unreachable from mainland China because the port, protocol, or destination IP become unreachable. These sites continue to be reachable from other locations outside of China. All attempts to involve local Chinese carriers have resulted in either no feedback or inconclusive responses with no real resolution.

Should this occur, you have the choice of either purchasing a China Premium Access solution, a ZIA Private Service Edge, or a ZIA Virtual Service Edge.

Certain applications slow down during peak business hours

Zscaler has observed applications hosted outside of China by major public cloud providers performing poorly. These providers continue performing well from other locations outside of China. We have been able to correlate some of these incidents to the overall political climate in China and abroad, as well as to engagements between the Chinese telcos and the cloud provider.

Should this occur, you have the choice of either purchasing a China Premium Access solution, a ZIA Private Service Edge, or a ZIA Virtual Service Edge.

The realities of troubleshooting connectivity issues in China

Troubleshooting network connections is a common occurrence around the world. In China, however, the experience takes on new complexities.

Due to Chinese regulations on network routing, organizations are prohibited from altering internet routes and paths themselves. If you are experiencing network issues, troubleshooting must be done with the help of the local service provider.

This often complicates or stalls the troubleshooting process. This is especially difficult if inter-carrier issues or the GFW is at fault. For business-critical traffic, customers can procure the ZIA Private Service Edge or ZIA Virtual Service Edge solution and use their existing connectivity to reach the internet.

Zscaler is committed to helping our customers troubleshoot and resolve all reported issues. Given the complexities and need to always involve the local ISPs, long wait times between updates and resolutions should be expected.

Leveraging ZIA from within China

International internet access from mainland China presents a unique challenge for most organizations. Zscaler partners with local ISPs, overlay IP network providers, and public cloud providers to develop a range of options for internet connectivity. We detail solutions from the most reliable based on premium private connections, to the least reliable using commodity internet access links within China.

In all cases, these solutions avoid sending traffic across the international link if its destination is within China. Tunneling all your traffic to a foreign data center such as Hong Kong is not only expensive, but it adds additional transit delay and unnecessary inspections. Instead, Zscaler recommends splitting off traffic destined for a China-based destination and routing it locally.

As a reminder, Zscaler is required to operate within the laws and regulations of its host country. ZIA is an overlay network, not a VPN nor a content provider. Zscaler cannot help you avoid traffic inspection or filtering. Compliance and enforcement of local laws and regulations is the responsibility of your organization and your users.

Zscaler China Premium Access offering

Zscaler has partnered with multiple partners in China to leverage their private IP backbones and points-of-presence (PoP) throughout China. These highly redundant, highly available networks are peered with all tier 1 carriers in China and all major carriers outside of China.

Overall, Zscaler offers three premium services in China:

- China Premium
  - Send traffic to a Zscaler data center hosted on a premium Chinese ISP that has access to both domestic internet in China and premium access to international websites and SaaS applications.
  - International traffic is protected with a Zscaler Service Edge in the local premium ISP.
- China Premium Plus
  - Send traffic to a Zscaler data center hosted on a premium Chinese ISP that has access to both domestic internet in China and a dedicated link to international websites and SaaS applications.
  - International traffic is protected with a Zscaler Service Edge in the local premium ISP.
- China Premium Underlay
  - Zscaler-managed premium network connectivity.
  - Direct traffic through the partner backbone to prioritize international traffic into and out of China.
  - Protect traffic by connecting from the partner cloud to a termination point at a Zscaler connection point anywhere throughout the world.

Premium Access+ with local routing and private international link

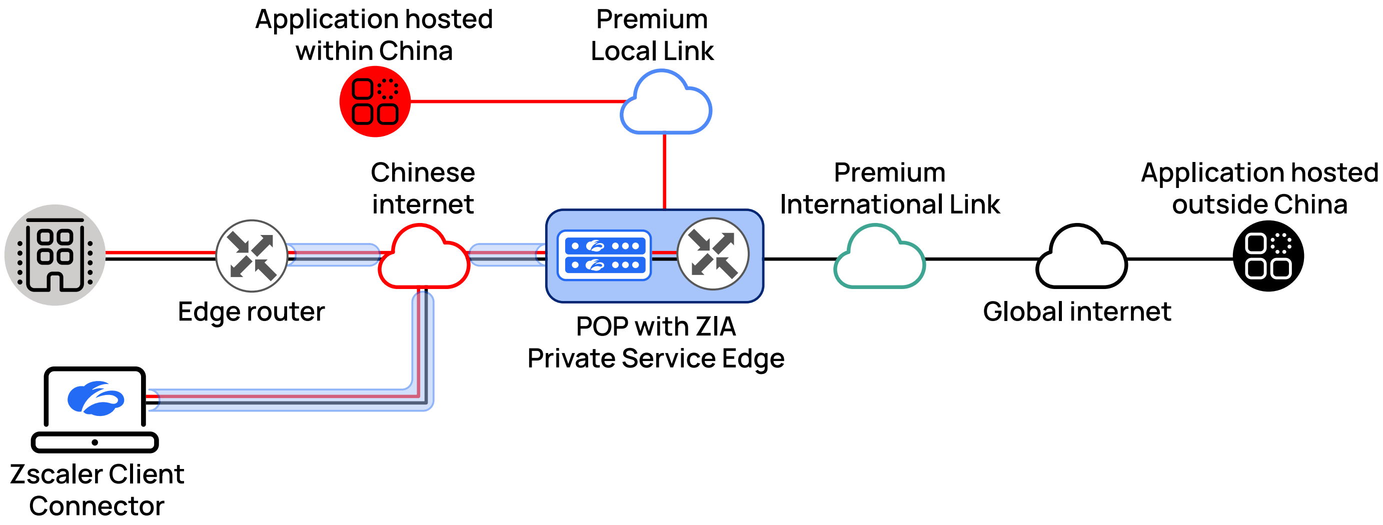

Application hosted within China
Premium Local Link
Chinese internet
Premium International Link
Application hosted outside China
Edge router
POP with ZIA Private Service Edge
Global internet
Zscaler Client Connector

Figure 2. Premium Access+ with dedicated ZIA Private Service Edge devices deployed at the Zscaler partner POP

Zscaler has partnered to deliver Premium Access+ in China. This is a dedicated and hosted solution for those organizations with the highest bandwidth and user counts. In this model, your organization subscribes to a dedicated ZIA Private Service Edge hosted in the partner network.

After your traffic has been inspected by the ZIA Private Service Edge, it is then routed across the partner's premium links. This can be the local premium link for traffic bound for destinations within China, or a private international link that handles all traffic for destinations outside of China via Hong Kong.

A typical organization that would subscribe to this service expects to have over 500 MB in sustained traffic from the organization.

Key benefits of this solution include:

- Customized for you – The number of ZIA Private Service Edge nodes, internet bandwidth, and redundancy requirements can be customized for customers. All devices are hosted for your organization in the partner PoP.
- Strong peering and performance – Direct peering with all China tier 1 and global tier 1 carriers. Availability and performance SLA with <1% packet loss guaranteed.
- Network resiliency – Diverse connections to different upstream providers for optimized connectivity globally.
- Experienced team – Zscaler and our partners have collaborated to serve several customers with high bandwidth and dedicated requirements for fortune 500 companies.
- Restricted application access – Customers can access applications that are usually restricted in China to facilitate business-critical communication. Besides the required application, access to all other applications is restricted similarly to GFW.

Under the Premium+ service terms and conditions, Zscaler discloses through our partner the name of the customer's Chinese entity information that uses the private link, as well as any whitelisting that was enabled.

Premium Access with local premium route and jointly managed ZIA Private Service Edge

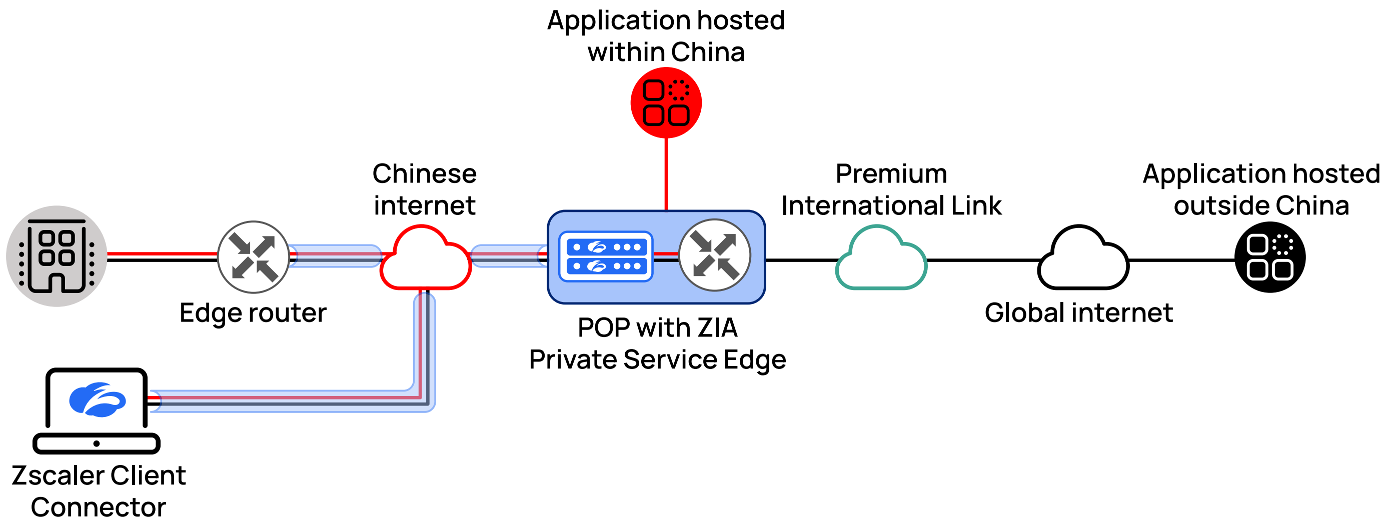

Application hosted within China
Chinese internet
Premium International Link
Application hosted outside China
Edge router
POP with ZIA Private Service Edge
Global internet
Zscaler Client Connector

Figure 3. Premium Access with ZIA Private Service Edge devices and local traffic routing

This model is co-built by Zscaler and our partners, using ZIA Private Service Edge devices deployed in partner PoP locations. In this model, the customer can use any edge provider and device that supports GRE tunneling to the ZIA Private Service Edge. This eliminates the need to change edge providers and simplifies routing.

The customers' traffic is forwarded across the GRE tunnel to one of the partner PoP locations. When the traffic reaches the PoP, the ZIA Private Service Edge inspects the traffic and applies policy. After inspection, traffic enters the partner's backbone network.

For traffic destined for a location inside of China, the partner forwards traffic across its China IP backbone. For international traffic, this crosses the partner's premium international backbone.

Key benefits of this solution include:

- Edge agnostic – Build tunnels from any customer endpoint to a ZIA Private Service Edge managed by Zscaler partners in China.
- Strong peering and performance – Direct peering with all China tier 1 and global tier 1 carriers. Availability and performance SLA with <1% packet loss guaranteed.
- Network resiliency – Diverse connections to different upstream providers for optimized connectivity globally.
- One-stop shop – Customers can achieve secure and optimized internet in China from a single managed service provider.

Zscaler China Premium Access with partner-supplied SD-WAN forwarding solution and ZIA Public Service Edges in China

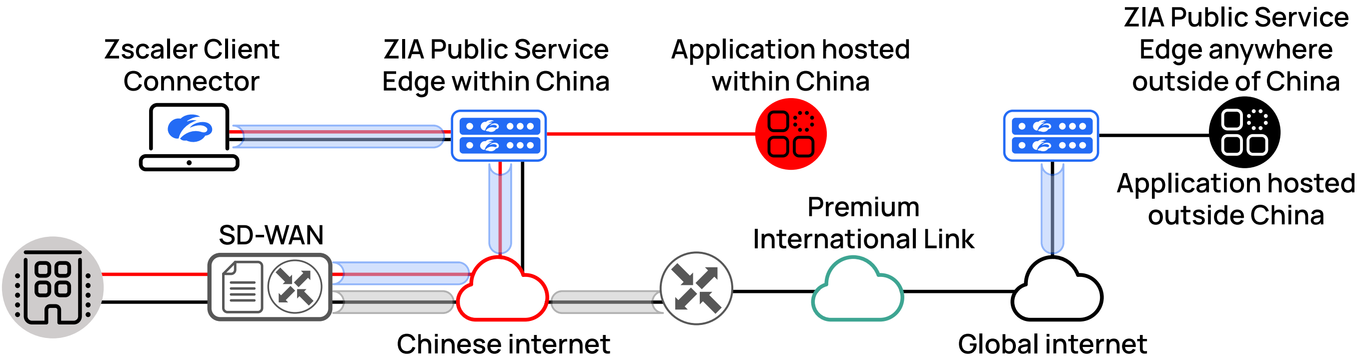

Zscaler Client Connector
ZIA Public Service Edge within China
Application hosted within China
ZIA Public Service Edge anywhere outside of China
Application hosted outside China
SD-WAN
Premium International Link
Chinese internet
Global internet

Figure 4. Premium Access with partner-supplied SD-WAN forwarding solution and ZIA Public Service Edges in China

In this model, the partner provides a CPE SD-WAN device at the customer's network edge. This device makes intelligent routing decisions, directing traffic to ZIA Public Service Edge data centers in both China and Hong Kong. The data center routing decision is driven by the traffic destination, and which is the most appropriate data center to service that request.

If the traffic is bound for a local destination within China, it is routed over a GRE tunnel to the nearest ZIA Public Service Edge in China. Our partners are closely peered with all tier 1 carriers in China and globally.

If the traffic is instead destined for an international destination, it is placed into an IPSec tunnel and forwarded to the partner backbone. The traffic is routed to the partner's international gateway of its premium international link, which experiences less than 1% packet loss within its backbone. Resilient upstream connections to global tier 1 providers provide connection redundancy.

This splitting of traffic ensures that China-bound traffic does not cross the international link. Instead, the traffic remains within the borders of China and is processed locally. This can be a huge cost savings for your organization by limiting what goes across the international link.

Key benefits of this solution include:

- Software defined – Manage and monitor all sites' performance from a centralized portal.
- Strong peering and performance – Direct peering with all China tier 1 and global tier 1 carriers. Availability and performance SLA with <1% packet loss guaranteed.
- Network resiliency – Diverse connections to different upstream providers for optimized connectivity globally.
- Smart routing decisions – Path select or prioritize certain applications based on network requirements.
- Turn-key solution for existing ZIA customers.

Understanding ZIA Private Service Edge and ZIA Virtual Service Edge

In some situations, using a ZIA Public Service Edge might not be available to your organization. These organizations typically have high bandwidth requirements, experience high latency when connecting to a ZIA Public Service Edge, or have geopolitical considerations.

In these situations, the Zscaler Zero Trust Exchange can be extended into your organization's DMZ using physical or virtual devices managed by Zscaler. You can lease and deploy either a physical ZIA Private Service Edge device, or a ZIA Virtual Service Edge virtual appliance in your network DMZ.

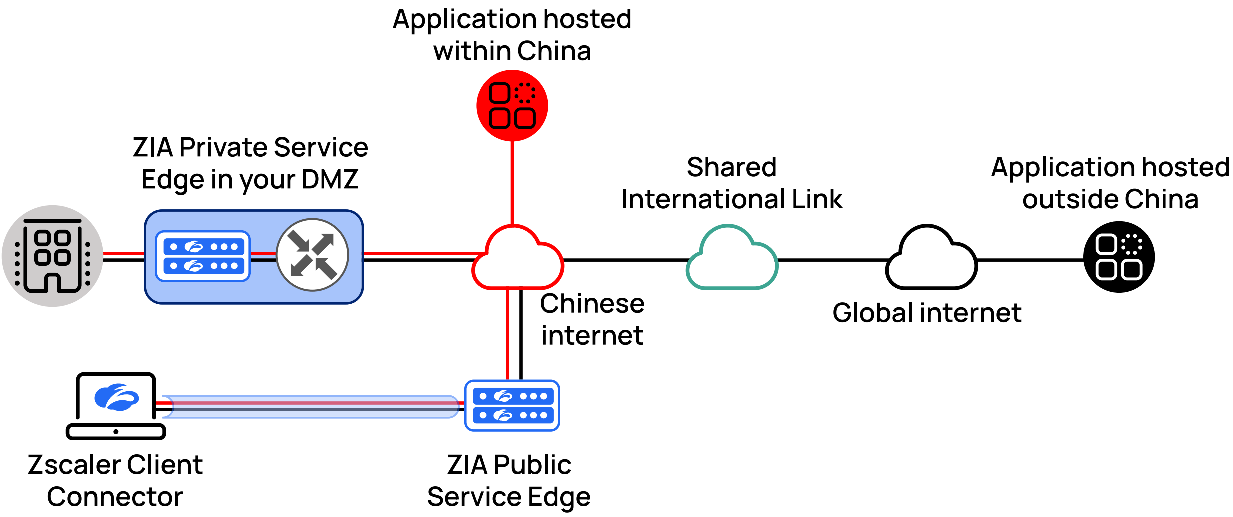

Application hosted within China
ZIA Private Service Edge in your DMZ
Shared International Link
Application hosted outside China
Chinese internet
Global internet
Zscaler Client Connector
ZIA Public Service Edge

Figure 5. ZIA Private Service Edge and ZIA Virtual Service Edge devices expand the Zscaler cloud into your organization

Your site traffic is forwarded to the ZIA Private Service Edge or ZIA Virtual Service Edge in your DMZ. Here, your traffic receives the same inspection and policy enforcement as at a ZIA Public Service Edge before leaving your network boundary.

Your legitimate traffic exits your organization already having been inspected and can be routed directly to its ultimate destination. You can use any available internet service provider to carry your traffic after inspection.

Both the ZIA Private Service Edge and the ZIA Virtual Service Edge require an additional subscription, and are leased devices. Contact your Zscaler representative for more information.

For more information on the ZIA Private Service Edge, see **About Private Service Edge** (**https://help.zscaler.com/zia/about-service-edge**).

For more information on the ZIA Private Service Edge, see **About Virtual Service Edge** (**https://help.zscaler.com/zia/about-virtual-service-edges**).

Maintenance of the ZIA Private Service Edge or ZIA Virtual Service Edge

When deployed, the ZIA Private Service Edge or ZIA Virtual Service Edge devices are monitored and managed by the Zscaler operations team. These instances are treated as an extension of the ZIA cloud and maintained and operated by Zscaler. After installation, the ZIA Private Service Edge or ZIA Virtual Service Edge should be a mostly hands-off operation for your staff.

To learn more about the shared responsibility model, see **Maintenance Support for Private Service Edge** (**https://help.zscaler.com/zia/maintenance-support-private-service-edge**).

Government licensing and Zscaler Client Connector

Zscaler Client Connector is a software agent that runs on user devices including Windows, macOS, Linux, iOS, and Android. This software agent connects your users to various services when they are away from your organization's offices. By automatically building tunnels to the nearest ZIA Public Service Edge device, your users' traffic is protected while roaming.

To do this, Zscaler Client Connector builds tunnels using ports 80 and 443, which are strictly regulated by the Chinese government. To use Zscaler Client Connector, your organization needs to obtain a license to use these ports prior to deploying Zscaler Client Connector. Zscaler encourages you to work with your local internet provider and legal teams to fully understand these requirements.

For more information on Zscaler Client Connector, see **What is Zscaler Client Connector?** (https://help.zscaler.com/z-app/what-zscaler-app).

Legal notice

Disclaimer: This document has been created by Zscaler for informational purposes only and is designed to try and help organizations understand Zscaler's position in China. Therefore, it should not be relied upon as legal advice or to determine how the contents might apply to you or your organization. We encourage you to consult with your own legal advisor with respect to how the contents of this document may apply specifically to your organization, including your unique obligations under applicable law and regulations. ZSCALER MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Zscaler product. You may copy and use this document for your internal, reference purposes only.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.