Zscaler™ in China

Connectivity and Service Expectations in Mainland China for Domestic and International Traffic
Zscaler provides connectivity for organizations with locations in mainland China. This Tech Note highlights the challenges related to internet connectivity and performance in mainland China, Zscaler’s stance on licensing, and best practices for providing the required internet connectivity for Zscaler customers in this region.

Zscaler legal stance in China

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. Simply, if Zscaler did not exist, the request, response, and content delivery would still occur.

In China, if the content provider is serving the content from mainland China, then the content provider would need an ICP license; if the content provider is outside of mainland China, it does not have to obtain an ICP license. Since Zscaler will be reaching out to providers through the “Great Firewall of China” (GFW), any restrictions on content providers will be observed.

It is the opinion of legal experts and partners that Zscaler is in compliance with Chinese regulations as long as we do not generate or serve content or offer additional encryption services. The responsibility to comply with Chinese regulations is on the employee and employer generating the requests and on content providers if they are in country.

Zscaler is constantly reviewing the dynamic legal landscape in China and reserves the right to take any measures necessary including shutdown of service.

Customers are strongly encouraged to have backup solutions such as Zscaler Internet Access (ZIA) Service Edge/Virtual Service Edge or other measures to ensure service continuity.

Note: Zscaler does not facilitate any bypass or subversion of Chinese laws and regulations. Zscaler cannot guarantee or influence connectivity performance between mainland China and international destinations.
Internet Connectivity

There are two primary telecom operators in mainland China: China Unicom and China Telecom. China Unicom covers the north and China Telecom covers the south.

Internet connectivity with mainland China is strictly regulated by the government, with sweeping laws banning many types of content and sites, and ongoing traffic inspection. Policies are enforced by the GFW, which controls access based on variables such as:

- Blocking of URLs and IPs (such as Google or Facebook)
- Alteration of DNS requests
- Applications (such as TOR)
- Keywords
- Other Variables – IPs, technologies, and other parameters not publicly disclosed

The policies can change without notice and, at any given moment, certain traffic can either be blocked entirely or discouraged by throttling bandwidth. Hong Kong and Macau are part of China but are currently largely exempt from these regulations and are outside of the control of the GFW.

We have observed that major events, like elections, holidays and internal political events cause erratic behavior with regards to performance and consistency of application reliability before, during, and after such events. An example of the complexity of this disruption can be found here.

Zscaler connectivity with China

Zscaler operates three data centers (DCs) in China: one in Beijing, one in Tianjin, and one in Shanghai. The Tianjin and Beijing DCs provide better connectivity for organizations connected through China Unicom, while the Shanghai DC is better for China Telecom connectivity. Connectivity should be tested during peak business hours.
It should be noted that Zscaler does not guarantee international connectivity or quality of the connections, and we have observed variance in quality and connectivity from our nodes to international destinations. This variance is sometimes positive and sometimes negative in terms of performance and availability.

Considerations:
• PAC files: as all connections go through the GFW and are subject to government policy, Zscaler cannot guarantee performance or availability.
• ZIA Service Edge/Virtual Service Edge requires access to port 80/443 for monitoring and updates. Such access may require the customer to obtain a government license.

Troubleshooting connectivity issues in China
Chinese regulations prohibit end users from altering internet routes and paths. Troubleshooting must be done with the help of the local service provider. This often complicates or stalls the troubleshooting process, especially if inter-carrier issues or the GFW is at fault. Zscaler is committed to troubleshooting reported issues, but long wait times between updates and resolutions are to be expected.

For business-critical traffic, customers can procure the ZIA Service Edge/Virtual Service Edge solution and use their existing connectivity to reach the internet.

China to international destinations observations
While operating in China, we have observed several behaviors of traffic originating in mainland China towards international destinations, especially during business hours. This applies both to customers attempting to connect to Zscaler DCs outside of China and to Zscaler Chinese data centers connecting to international destinations.
• Certain ports, protocols (IPsec, GRE), or IPs are unreachable – At times or in general, certain international destinations become unreachable from mainland China but are reachable from other locations. All attempts to involve local Chinese carriers result in no feedback or inconclusive responses with no real resolution. In such cases, customers frequently fall back on a private solution such as ZIA Service Edge/Virtual Service Edge/network solution for the impacted application(s).
• Certain applications slow down during peak business hours – We have observed applications hosted outside of China by providers like Amazon, Akamai, Google Cloud, Microsoft Azure, or others performing poorly at times while performing well from other locations. We have been able to correlate some of these incidents to sales motions and commercial negotiations by large Chinese telcos and the particular cloud provider. In such cases, customers frequently fall back on a private solution such as ZIA Service Edge/Virtual Service Edge/network solution for the impacted application(s).