Skyhigh Security SSE in China

Dated: January, 2026

Understanding China's Regulation

Investigation has shown that, to operate any cloud service within China, a company needs to obtain a governmental license. These are called Internet Content Provider (ICP) licenses. These are required to legally operate a website within China.

Generally, these aim at operating a website and are split into two separate licenses:

- ICP Commercial license
- "Bei'an", which is the filing for a non-commercial offering

A commercial license will only be provided to companies that are:

- Chinese-owned businesses that have a Chinese business license
- Joint-venture companies

The definition of what constitutes a website is unclear and with that, to be sure, a license should be obtained regardless of the nature of the website or webservice. Only the license will enable a company to get access to hosting companies to deploy servers or rent servers.

In many instances, services of international companies are marketed under their brand but are operated as a standalone cloud by a Chinese company on their behalf. That enables compliance with the ICP requirements but also leads to giving way control on the service, which is the reason why several CSPs do not offer the same feature set in China.

Amazon's Cloud is operated by Beijing Sinnet Technology Co., Ltd. and Ningxia Western Cloud Data Technology Co., Ltd.

- https://aws.amazon.com/china-gateway

Microsoft's Azure and O365 is operated by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

- https://learn.microsoft.com/en-us/azure/china/overview-operations

In addition, China passed the Cybersecurity Law of the PRC ("CSL") in June 2017 with a review in 2020. That law regulates data sovereignty, cross order transactions and includes the right for assessment of the service by the government. The CSL is not very clear on how the assessment is conducted and leaves room for interpretation.

All that ambiguity in ICP licenses, the governmental right to audit under the CLS regulation under unknown circumstances has led Skyhigh Security to the conclusion to not offer its SSE Cloud service in China.

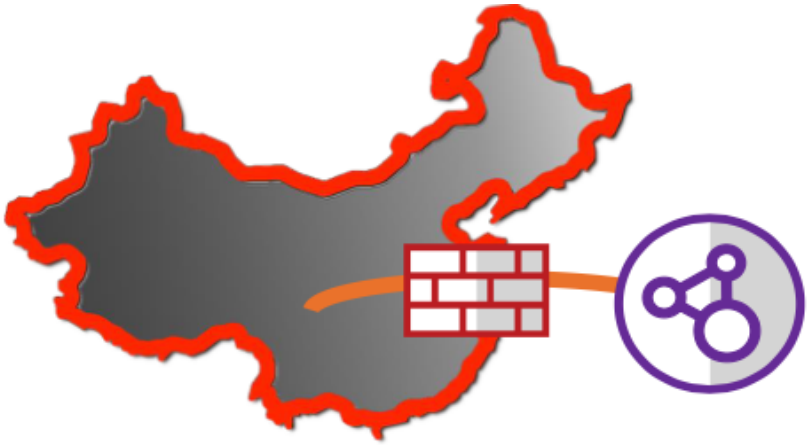
- Skyhigh Security doesn't want to risk putting customers' businesses and its own service at risk and on that basis has decided not to offer the Cloud SWG, Private Access or Cloud Firewall in mainland China.
- Similarly for CASB, Skyhigh Security does not support Sanctioned SaaS Cloud Services based out of China and Shadow IT if the customer's web gateways are based in China. (see details in subsequent sections)

Connectivity to International Cloud Services From Within China

Independent of Skyhigh Security offering a service in China, customers have reported issues while connecting to international locations from within China.

While China is allowing a certain freedom for web data within the virtual borders of China, international connections are subject to a higher scrutiny. The instrument of control is casually referred to as the Great Chinese Firewall. This nation-wide edge gateway applies several controls to data leaving the country. The controls applied to the traffic include active filtering. The active controls include, but not limited to:

- IP blocking
- URL Filtering
- DNS spoofing
- Filtering and redirection
- QOS
- Packet forging and resets
- Man in the middle attacks for TLS connections



The criteria under which these are applied are unknown and not documented publicly but generally seem to apply to international data transactions.

For example, customers have reported that they get throttled (QOS) first when accessing an international Internet destination and then have been receiving TCP resets on any outbound connection afterwards for a certain period.

These network level controls are independent of Skyhigh Security's offerings and are part of the regulations of the Chinese government. Customers are encouraged to familiarize themselves with the respective laws and regulations in China.

SSE Options For Customers

As previously indicated, the services in mainland China are operated by licensees of the respective CSPs. As such not all functionality is available on the platforms in China, as that would require licensing proprietary or even protected technology to the companies operating the service.

Generally, Skyhigh Security's services, CASB, Private Access, SWG or Firewall are subject to connections to international instances outside of mainland China and as such are subject to scanning by China's Internet protection system, the Golden Shield aka. China's "Great Firewall".

Skyhigh Security's offerings are designed to work with the general version of the respective cloud services and are not explicitly tested against the China specific implementation of the CSP. As such, Skyhigh Security cannot guarantee that all options of the SSE product portfolio are generally working with the Chinese instances of the CSP.

This does apply to API level integrations, reverse proxy connections or data in the cloud registry. All of these combined with the licensing ambiguity as mentioned before **has led Skyhigh Security to the conclusion to not offer its SSE Cloud service in China.**

Options For SWG, ZTNA (Private Access) Or FWaaS

With that customers can filter traffic within China using the rich feature set of the SWG appliances. Customers can even set up a world-wide appliance cluster if deployed in a hybrid configuration so that policy is synced into these instances in customers provisioned cloud instances in China.

Options For CASB

Skyhigh supports a fully cloud based CASB solution – however, it **does not support Sanctioned SaaS Cloud Services based out of China and Shadow IT if the customer's web gateways are based in China**.

However, several customers who have operations in China use the Skyhigh CASB solution in the following ways:

(1) Shadow IT: If all traffic logs are pushed to a global instance of their Firewall/Proxy/SIEM located outside of China. Skyhigh CASB can connect to this SIEM and pull logs to provide visibility into all cloud usage.

(2) Sanctioned SaaS support: The admin tenant of the cloud service is located outside China. For example, if an Office 365 customer has users in China but has the admin tenant in the United States, then Skyhigh can connect to this admin tenant and support all sanctioned SaaS use cases, like DLP, Activity Monitoring.