Advantage | How Do Enterprises Navigate China's VPN and SD-WAN Ban?

Meta Data

Title Tag: How Do Enterprises Navigate China's VPN and SD-WAN Ban?

H1: How Do Enterprises Navigate China's VPN and SD-WAN Ban?

Meta Description: China's VPN ban presents obstacles to global enterprises. Find out how to stay connected and compliant with licensed MPLS, VPN, and SD-WAN solutions.

Slug: how-enterprises-manage-china-vpn-ban

Blog image header:

- https://unsplash.com/photos/a-city-skyline-at-night-with-a-bridge-in-the-foreground--bOqztU8ndI

Introduction

Before 2018, Virtual Private Network (VPN) and Software-Defined Wide Area Network (SD-WAN) services were the primary connectivity solutions for circumventing the Great Firewall—the robust framework of internet access restrictions in China.

Then, the 2018 ban on unregistered VPN and SD-WAN services in China forced global enterprises to find new methods for maintaining operational continuity and connectivity.

Read on for updates on compliance specs and an overview of China’s current regulatory environment. You’ll discover the strategies, technology solutions, and security measures that international enterprises are using to successfully navigate this unique landscape.

What’s changed since the original VPN and SD-WAN ban in China?

Since China’s VPN ban blocked SD-WAN and VPN traffic over six years ago, the government released increasingly punitive regulations in 2021. The state blocked more VPNs in 2022 and is now enforcing these regulations more broadly.

For example, the 2020 Foreign Investment Law requires international companies to follow the same strict laws as domestic ones. The Great Firewall hinders access to global trends, research, and best practices, potentially stifling business innovation. It also persists in the creation of ongoing latency and security concerns.

But it’s not all bad. In March 2024, the Cyberspace Administration of China (CAC) relaxed cross-border data transfers and simplified security assessments while extending their validity.

Compliant connectivity solutions to China’s VPN and SD-WAN ban

Thankfully, global companies *can* use VPNs and SD-WAN services—they just have to jump through some hoops.

Let’s review how enterprises legally leverage these connectivity solutions.

Government-approved VPNs

Enterprises must complete a range of documentation and follow strict guidelines to get a VPN license from the government.

Companies must obtain and register their VPN through one of the ‘Big Three’ state-approved providers:

- China Telecom
- China Unicom
- China Mobile

Businesses can only implement VPNs through MPLS or SD-WAN protocols (not IPsec tech). They must proactively block illegal sites and use VPNs strictly for internal business.

Multiprotocol Label Switching (MPLS)

MPLS is an overlay technique that leverages diverse protocols to transfer data through physical circuits on a private network. This hardware-dependent technique is a viable and reliable WAN alternative, as China's VPN ban doesn't affect site-to-site connectivity across MPLS. Unfortunately, it's costly and less flexible than SD-WAN.

Enterprises purchase MPLS solutions from a Big Three carrier, which has the proper licensing. Businesses then register solutions with the government and create physical resources—data centers, offices, and physical circuits—to implement them.

SD-WAN with local partners

SD-WAN blends software-defined computing with WAN tech to interconnect IT infrastructure across the globe. This streamlined, cloud-friendly solution uses existing provider networks and is less expensive than MPLS. It's also less reliable and less secure, although using it through a VPN enhances security.

As with VPNs, the 2018 ban disallowed *unregistered* SD-WAN solutions. However, enterprises can implement compliant SD-WAN solutions by partnering with Chinese telecom providers that comply with regulations and have a license from the state.

Strategies for maintaining business continuity in China office locations

Despite rising challenges, many global companies are successfully maintaining continuity. China ranked fourth in Foreign Direct Investments (FDI) in 2023.

In fact, McKinsey's research shows that revenue growth rates for high-performing multinational companies in China have expanded in recent years.

Let's dissect some strategies businesses are using to find continued success.

Data centers in China

Establishing data centers on-site minimizes latency, optimizes performance, and streamlines compliance with strict data-localization requirements.

Enterprises avoid disruptions, reduce delays, and circumvent complex cross-border transfer regulations by keeping data inside China.

Cloud connectivity

Cloud-based solutions like IaaS, SaaS, and PaaS help with compliance while ensuring connectivity and reliable communications with Chinese offices.

These solutions are relatively scalable and cost-effective, but most foreign companies aren't eligible for the necessary licenses. Global enterprises must work with one of the Big Three, another major Chinese provider, or an international partner that offers compliant on-site frameworks and secure application access.

These services take many forms, from direct cloud connectivity to hybrid solutions.

Network optimization

To mitigate latency and bandwidth limitations in China, organizations use performance monitoring software and test applications for efficiency. They leverage **Content Delivery Networks (CDNs)**, optimize their **Domain Name Systems (DNS)**, and establish private connections through MPLS or a **Dedicated Internet Access (DIA)** provider.

For the best results, enterprises engage trusted partners with localized expertise.

Security considerations for enterprises in China

Due to stringent compliance regulations and increased cybersecurity risks—from state-sponsored hacking campaigns to vulnerabilities via tool restrictions—operating in China demands robust security considerations.

Compliance

International companies must comply with relevant international standards *and* strict local laws like **China's VPN and SD-WAN ban**.

Chinese regulations

The **2017 Cybersecurity Law (CSL)** outlined specific data-localization requirements and afforded authorities augmented monitoring capabilities. The **2021 Data Security**

Law (DSL) tightened security system requirements, required data-protection officers for sensitive information, and presented fines for large-scale failures.

The Personal Information Protection Law (PIPL) became more stringent in 2021. It now requires businesses to obtain user consent, notify authorities when transferring data out of China, and document data-collection practices explicitly.

The Network Data Security Management Regulations—which go into effect in 2025—outline updated cybersecurity, risk assessment, emergency response, and data-storage regulations.

International regulations

Companies must also follow a range of international standards, such as:

- **GDPR** (for general consumer data)
- **HIPPA** (for healthcare data)
- **SOX** (for general financial reporting)
- **ISO/IEC 27001** (for general information security management)
- **PCI DSS** (for payment card data)

Data security solutions

Due to stringent laws and privacy concerns, enterprises adopt advanced security measures that protect sensitive information, ensure secure operations, and avoid compliance issues.

Examples include:

- End-to-end encryption solutions
- Data masking
- Secure data transfer protocols
- Access controls
- Regular risk assessments

Companies must also implement proactive **threat-monitoring systems** and reactive **disaster recovery plans**. Proactive threat-detection solutions mitigate cybersecurity risks by stopping breaches at the source, while robust incident-response protocols minimize damage if cyber attacks occur.

Engage a trusted partner with local China telecom knowledge

Third-party experts with experience navigating the complexities of China’s market can better address connectivity and compliance issues.

For this reason, many international enterprises engage connectivity providers that offer consulting services, localized support, and tailored solutions. Adopting a trusted partner helps foreign companies mitigate the legal and financial risks of operating in China.

Conclusion: Maintain secure and reliable connectivity in different regions

China’s regulatory environment presents unique challenges for international operators, and tightening restrictions since the VPN and SD-WAN ban continue to present complex problems for global enterprises.

But with the right strategies, multi-location enterprises can maintain reliable continuity, security, and connectivity in China. Many organizations adopt a trusted connectivity partner with expertise to succeed in this challenging market.

Let Advantage guide you through the complexities. We offer advisory support and tailored connectivity services to help you navigate regional regulations while ensuring seamless continuity.

Connect with our experts today to start optimizing your networks and safeguarding your operations in Asia.

Recommended reading (Helpful links)

- What is the Role of MSPs in Global Enterprise Connectivity
- How to Save Time Researching Telecom Providers in Other Countries
- Enterprise IT Checklist for Nationwide and Global Expansion

LinkedIn Posts

Post Copy 1:

Maintaining business continuity in China? It's possible, even in the face of strict VPN and SD-WAN bans.

Explore how global enterprises are leveraging compliant solutions like government-approved VPNs, localized SD-WAN partnerships, and cloud strategies to stay connected.

Secure your operations and optimize performance while navigating China's regulatory challenges with ease.

📖https://www.advantagecg.com/blog/how-enterprises-manage-china-vpn-ban

#GreatFirewall #ITSolutions #CloudConnectivity

Post Copy 2:

China's evolving regulatory landscape presents unique challenges for multinational enterprises. The VPN ban in 2018 and subsequent updates have transformed how businesses operate.

From MPLS to compliant SD-WAN solutions, and enhanced security measures, companies are getting creative to maintain business continuity. 🔒

If you're ready to tackle China's complex internet framework with confidence, we've got the insights you need.

➡️ https://www.advantagecg.com/blog/how-enterprises-manage-china-vpn-ban

#GreatFirewall #DataSecurity #TechStrategy