VDMA Facts Sheet

Competence Center Industrial Security

Status Quo VPN & Data Exchange in China

Update with state of knowledge March 2020

Notes

With this fact paper, experiences of VDMA members and nicos AG are brought together in order to jointly contribute to an understanding of the topic "VPN and China". This paper is exclusively intended for information to VDMA member companies and only represents the experiences from the operation of VPN as well as from discussions with Chinese carriers and legal advisors of nicos AG regarding the development of the cyber security regulation in the People's Republic of China.

Summary

With the regulation of Internet access services adopted in 2017, Chinese authorities have tightened the regulation of encrypted data transmission to and from China[1]. The implementation of the regulatory measures was postponed until March 2019 due to economic and political concerns. Since then, companies have had to use Internet access from approved providers if cross-border encrypted data transmission is to continue to be used for business in compliance with the law.

According to the regulation, multinational corporations are allowed to use cross-border VPN connections if they directly lease international dedicated lines (including VPNs) for this purpose[2]. If VPN connections to foreign countries are established via standard Internet accesses, data transmission is promptly interrupted - up to a permanent blockade.

VDMA recommends setting up a dedicated line for cross-border encrypted data traffic of machine data. The data transfer of individuals and IT systems should be separated, if possible. Internet access for employees is to be reduced to operational purposes, unauthorized VPN connections should be prevented. The business Internet services of China Telecom and China Unicom have proven to be quite reliable for this purpose. VPN connections over MPLS lines are very reliable, but also very expensive.

Currently (as of March 2020), no tightening of the regulation of encrypted connections can be identified. The focus of regulation is shifting from the operation of VPNs to the official examination by authorities of what kind of data is being transmitted (keyword "important data"). This is particularly true for sensitive data, personal data or data that is important for the Chinese economy.
According to information from nicos AG's talks with Chinese providers, the market consolidation of so-called "gray line providers" (providers who have provided individuals with unauthorized access to blocked services via VPN & Apps) has been completed.

[1] http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html (call date: 19.01.2018)
[2] See EU Chamber of Commerce in China: ICT Working Group Position Paper 2019, Kapitel “Internet Access”

VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main, Germany
Phone +49 69 6603-1360
E-Mail informatik@vdma.org
Internet industrialsecurity.vdma.org
Register of associations
AG Frankfurt/Main, No. VR4278

Informatics Department

Department head:
Prof. Claus Oetter

President:
Carl Martin Welcker

Chief Executive Officer:
Thilo Brodtmann

Legal notice

The situation regarding cyber security in China is anything but stable. Although the Cyber Security Law has been passed, most of the legal regulations necessary for its implementation are still being voted on.
Please note that the legal situation in China can change very quickly and actions that are legal today may be illegal tomorrow. We therefore recommend that you regularly review your own actions to ensure that they comply with the law.
The Legal Department of VDMA will be pleased to name appropriate lawyers for this purpose.

The findings and recommendations in this fact paper were formulated based on non-official translations of currently available drafts and adopted laws and are provided for information purposes only. Under no circumstances can a claim to completeness and accuracy be derived. The present document is therefore in no way to be understood as legal advice. It is expressly pointed out that lawyers with appropriate expertise should be consulted for a final assessment of the specific facts.

Additionally, this document was translated from German into English using an AI-based service. Although we reviewed its translation, there still might be misleading wordings.

Internet vs. China Internet

With the permanent connection of China to the Internet in 1994, regulatory orders were introduced early on. The first *regulation,* dating from 1994 ("*Regulations of the People's Republic of China for Safety Protection of Computer Information Systems*"), already referred to the use of the Internet in compliance with state interests.[3]

Also in the late 1990s, the technical course was set for a far-reaching censorship of Internet access in China. Since then, the so-called "*Great Firewall of China*" (GFW or GFC) has been operated by the "*National Computer Network Emergency Response Technical Team Coordination Center of China*" (CNCERT/CC) under the umbrella of the "*Ministry of Industry and Information Technology"* (MIIT). The specifications as to which websites and keywords should be blocked or filtered come directly from the Chinese government. The primary objective is *national security*, which means in particular the protection and preservation of China's social structure. It is propagated that both state and citizens should be protected from negative, external influences. One unofficial aim of the new regulation is to massively restrict all anonymous VPN services to prevent individuals from an uncontrolled entry into the "free Internet".

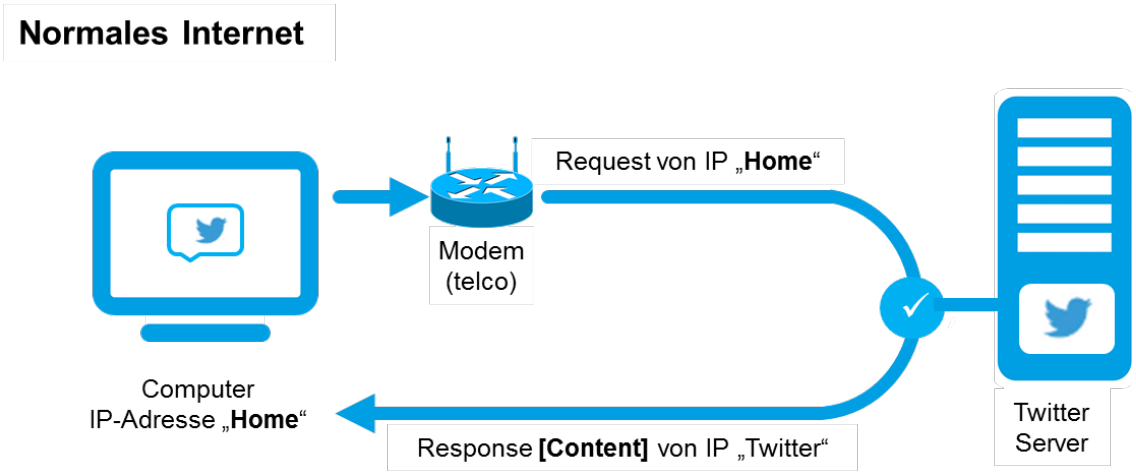

Figure 1: Web pages like Twitter.com are loaded when the computer sends a request to the server. Together with the requested data, the server's own IP address is sent back. The website is reachable. (Source: nicos AG)

Normal Internet connections are not filtered by telecommunications providers in accordance with the principle of network neutrality. The German Bundesrat considers such non-discriminatory access to the Internet to be necessary in order to "*guarantee the equal and unrestricted participation of citizens in the open Internet as a central medium of our information society*"[4]. In principle, a website visit is neither blocked nor filtered (Figure 1).

[3] Cf. (Chen & Yang, 2018), S. 50.
[4] http://www.computerundrecht.de/0689_13_B.pdf

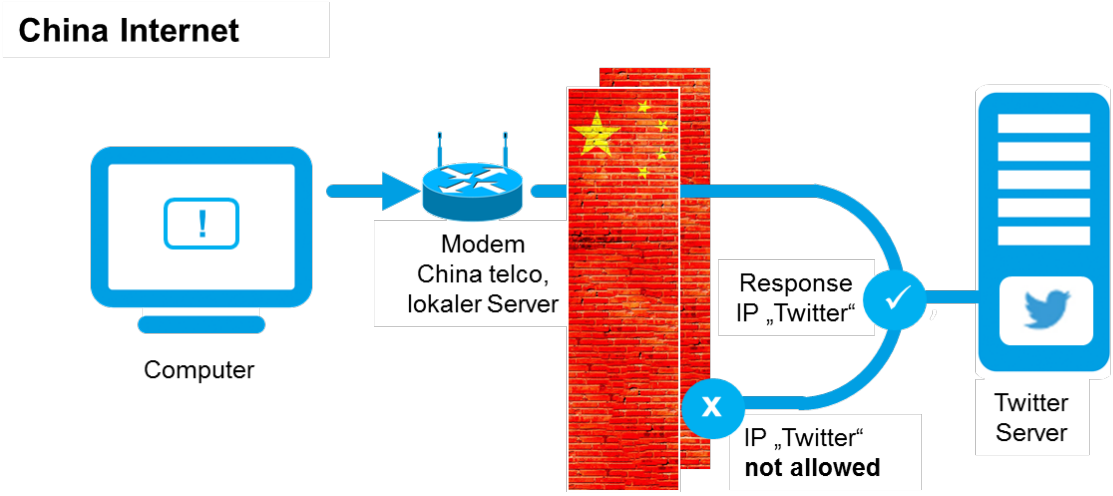

Figure 2: The "Great Firewall China" filters and blocks "prohibited" content that flows between the local servers (China Mainland) and overseas servers. Replies from IP addresses of certain services are not allowed and therefore do not reach the local computer. (Source: nicos AG)

Access to services and websites from China is restricted by the Chinese firewall. Technically speaking, all requests are possible, but data transfer from known Internet addresses (IP addresses) registered in the firewall is blocked (Figure 2). Since the system is based on a "blacklist" of Internet addresses, this system must be kept up to date by the authorities with a high maintenance effort. Several VDMA members are subject to such a blockade of their source IP address outside China Mainland every year, without any possibility to lift the block. One should remember that any blocking of IP addresses in the Chinese firewall is sustainable. These blockades therefore have a particular effect on companies' fixed IP addresses and static connections.

Bypassing access restrictions with VPN solutions

Both private individuals and companies worldwide use VPN applications to ensure confidential communication with services and companies. The protection of personal data, confidential information and company know-how is the focus here. To this end, Chinese citizens, expats and business travelers have in the past repeatedly sought ways and means to secure their connections. As a rule, VPN services are used for this purpose, which both ensure the confidentiality of data and make it possible to circumvent the blocking of services in the Chinese firewall. This blocking circumvention is generally illegal under Chinese law and will be sanctioned accordingly. For example, Chinese authorities block unlicensed connections after a short period of time, especially if illegal use is suspected.

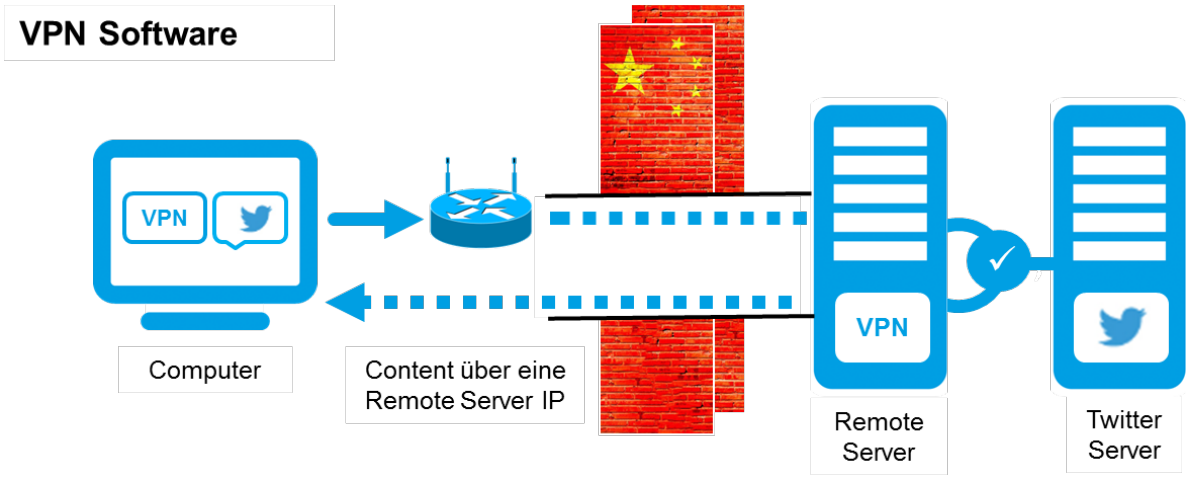

Figure 3: The VPN software is installed on a local computer in China and a remote server outside China and establishes an encrypted tunnel between them. To connect to Twitter, the data is sent from the local computer through the encrypted VPN tunnel to the remote VPN server. This server establishes the actual connection to the Twitter server. The returned encrypted data is not recognized as Twitter data by the firewall and is therefore not blocked. (Source: nicos AG)

The technologies, both for bypassing the Chinese firewall and blocking encrypted connections, have been playing cat-and-mouse for years.

Blocking of VPN by Chinese service providers

The Chinese authorities have recognized that efforts to technically prevent encrypted connections are not generally effective. For this reason, the new regulation of Internet access services now obliges providers to block the corresponding VPN services or completely shut down Internet access if they become aware of illegal use.

Affection of VDMA member companies

Since German but also other internationally active companies usually exchange data with their branches in China via encrypted connections (VPN), these connections can also be "regulated" or shut down.

In the past, VDMA members have repeatedly been affected by permanent shutdowns or blockades in the Chinese firewall:

- Blockade of the German IP address(es), these are no longer accessible from China
- Slowing down of encrypted connections, so that services (e.g. ERP connection) become unusable
- Shutdown of the Internet access in the Chinese branch office by the Chinese provider
- Disabling or blocking of mobile Internet access
- Blocking of encrypted connections (VPN) to services outside China

Shutdowns or blockades are permanent and have occurred regularly in the past for one of these two reasons:

- Employees of the company used encrypted connections to access Internet services or portals not permitted in China (e.g. Twitter, Facebook);
- The company operated a non-licensed VPN service, e.g. SSL-VPN, to cost-effectively encrypt data transmission to the head office abroad (Germany).

It should be noted that several member companies were able to establish and use VPN connections, some of which were usable for a very long period of time, without any problems. However, every time important dates, events or anniversaries (from the point of view of the Chinese government) come close, a targeted clean-up of previously tolerated VPN's takes place. Examples of such critical Chinese dates are:

- Meetings of the National People's Congress in March (recently on 5 March 2019)
- Anniversary of the protests by Chinese students in June (Tiananmen, 4 June 1989)
- Protests in Hong Kong (September 2019)

Legal requirements from the Cyber Security Law

To ensure the technical implementation of a reliable data exchange between Germany and China, machine and plant manufacturers must ensure that the technical measures are embedded in necessary organizational measures.
In particular, the possibilities for secure, cross-border networking are limited by complying with requirements arising from the Chinese Cyber Security Law.
The Cyber Security Law (CSL) focuses on national security, the protection of Chinese IT infrastructures, data protection and national sovereignty. It formulates

- Import restrictions for security-related products,
- Requirements for the secure operation of IT networks,
- Restrictions for data export, and
- Provisions on data protection.

VDMA has published an information sheet on the Cyber Security Law.[5]

[5] https://www.vdma.org/v2viewer/-/v2article/render/22344784 (retrieval date: 11.05.2018)

The obligation to store data locally means, for example, that the export of data is only permitted after passing a security check. It must be credibly demonstrated to a commission of experts why this export should be necessary for business activities. The security check is carried out on behalf of an "*Office for Security Verification*" under the "*Commission for Security Verification*" established by the China Cyberspace Administration (CAC) through tests and inspections on site. The check is based on the criteria of legality, necessity and legitimacy as well as the assessment of the risk factors arising from the data transfer. The results of the audit are presented to a committee of experts for decision.

The security check is accompanied by technical requirements for the transmission technology. For example, only products approved in China may be used. Products whose cryptographic procedures for data transmission have been approved by the OSCCA.[6]

All above has an impact on the technically legal implementation and long-term operation of the VPN connection.

[6] OSCCA: Office of the State Commercial Cryptography Administration

Implementation recommendations for VPN

In the following, you will find a summary of the legal and technical recommendations by VDMA, which should enable member companies to operate a reliable cross-border data exchange.

Operational recommendations

- Make it a board issue - it does not belong to IT.
- Appoint an IT security officer to control and monitor the organizational and technical implementation. This person may well be located in Germany.
- Take advantage of local companies in China that can help you with the technical implementation. This can also be a German service provider with experience in setting up cross-border connections.
- Check whether data transfer is necessary for the operating process.
- Find out which data is considered "important" or "sensitive" and could therefore be subject to local data storage requirements.

Technical recommendations

- Use two technically discrete lines for local Internet access and cross-border VPN to separate employee data transmissions from those of the IT systems.
- Use web filters to prevent the private use of the Internet and VPN to prevent your connection from being blocked.
- Use an officially licensed line for important IT systems or cross-border data exchange with increased availability for business customers.
- Depending on the availability requirements for VPN connections, VDMA suggests using officially licensed offers for “Industrial Internet” from
    - China Unicom (AS9929, no restrictions so far) or
    - China Telekom Global Internet Service (AS4809, minor restrictions) or
    - Dedicated MPLS lines (no restrictions, highest availability, expensive).
- Clarify in coordination with your service or technology provider to what extent approval of software or hardware for encrypted data transmission is necessary and has been submitted or granted by its manufacturer.

Data specific recommendations

- Store China-generated data in China if you have not applied for the appropriate release or permission to transfer or store data abroad.
- Use globally recognized partners for cloud services with an endpoint in "Mainland China" (not Hong Kong). Licensed partners must ensure the necessary approvals themselves, ask for corresponding documentation of such approvals.

Experience of nicos AG

"nicos AG as a managed service provider in the areas (WAN and security) has many years of experience in networking international locations of its customers. According to our experience, performance problems and blocking of connections to and from China have been the norm for many years. If a connection is blocked, it is not controllable, so that in these cases we work out individual alternative solutions with licensed providers for our customers in order to restore the connection of the locations as quickly as possible. For this purpose, we maintain very close relations with the carriers and our legal advisors. We are in constant exchange in order to be able to react quickly to new developments and to avert customer damage.
According to our information to date, no changes regarding blocking activities have occurred since the conclusion of the regulatory measures or since 1 April 2018. This supports our assumption that the regulatory measures primarily relate to VPN services offered by "gray line providers", which are used by individuals and do not focus on networks for cross-border corporate communication. According to the latest findings from the talks held in December 2019, a shift in focus towards the content and necessity of the data transmitted can be identified. (Keyword: data protection, data privacy)
Based on our experience, the risk of a connection failure can be minimized by using MPLS lines. However, since this is a high-priced solution compared to internet-based VPN connections, it is recommended to use this technology primarily for (time-)critical data communications.
A further reduction in the risk of breakdowns can be achieved by implementing redundancies regarding leased lines and its providers.
Generally, companies in China are advised that access to "prohibited content" should be prevented for employees of local companies ("[...] It is when users are "going" to these "unapproved" sites, that the Chinese government blocks all the traffic"[7]).
About the requirement of official approvals for the use and application of cryptography products in China, we recommend that you contact local lawyers to obtain legal certainty.
We are pleased to be available to VDMA members as the specialists of nicos AG for the setup and operation of Chinese and of course worldwide encrypted data connections."

[7] Nathalie Elizeon (Globalinternet; Partner of nicos AG), by e-mail of 20.03.2018.

Contact VDMA in China

Claudia Barkowsky
VDMA Liaison Office China (Beijing)
+86 10 87730212-808
claudia.barkowsky@chinavdma.org

Contact person of nicos AG

Axel Metzger,
Board of Directors
+49 251 98633 5102
ametzger@nicos-ag.com

Jost Bertels
Carrier Manager Access Solution Center
+49 251 98633 5509
jbertels@nicos-ag.com

Udate - China VPN Faktenpapier VDMA-nicos final ENGLISCH.docx

16.04.2020

Contact person at VDMA (Frankfurt)

Oliver Wack
Department Foreign Trade
+49 69 6603-1444
oliver.wack@vdma.org

Hermann Wegner
Department of Technology, Environment and Sustainability
+49 69 6603-1899
hermann.wegner@vdma.org

Daniel van Geerenstein
Law Department
+49 69 6603-1359
daniel.vangeerenstein@vdma.org

Steffen Zimmermann
Competence Center Industrial Security
+49 69 6603-1978
steffen.zimmermann@vdma.org