VIPRINET AND SECURITY

China and the USA mutually allege each other to bring router technology on the market that is equipped with backdoors for the purpose of economic espionage. Due to the NSA scandal, it is unquestionable that, even with network providers, confidential data is no longer secure. Companies as well as commoners find their confidence shaken; the State is unable to cope with this problem. Who can you trust now?

We are Viprinet, a router manufacturer developing and producing in Germany. The bug-proof end-to-end encryption of our VPN routers is entirely in your hand, and only you have the key. Our products are free of any backdoors, and we do not cooperate with any intelligence agencies.

To connect your company sites securely with each other, our routers use several reasonably priced consumer media like ADSL, UMTS/3G, or LTE/4G bonded together. Here, the data is encrypted and divided up onto the different links. Owing to this risk distribution onto several access networks, your site-to-site connection also becomes highly reliable, at low running costs - and even in the most remote areas or in mobile usage scenarios.

In the following, we'll explain in detail why you can unconditionally trust us and our products:

1) No back doors to Viprinet products

Viprinet does not provide intelligence agencies in any jurisdiction with special access to Viprinet products.

Should an intelligence agency or a secret court order attempt to force Viprinet to implement a back door in any Viprinet product, we pledge to inform all our customers in that country if legally possible, to immediately cease pursuit of new business in that country, and to withdraw from that country at the earliest opportunity.

2) Total control over product chain due to “Made in Germany”

It has to be assumed that hardware produced in the US but also in China is delivered with backdoors ex works. Only seldom, alleged European manufacturers are completely in control over the production chain for their products. Backdoors can thus be contained in products even without the manufacturer knowing about it. For IT security products produced in the US, it has to be assumed judging by the current state of facts that they contain backdoors for the NSA. For products of Chinese manufacturers, a backdoor for Chinese intelligence agencies has to be assumed.

In Germany, there luckily are no kangaroo courts that could decree backdoors in products. Also, no such ambitions of German intelligence agencies have yet become public.

Regarding their software, our products are developed entirely in Germany. Our source codes are protected from external access in an almost paranoid way. The hardware for our router products is also developed and produced entirely in Germany.

3) Paranoid security architecture

From design, our devices are split up internally in a “clean” and a “dirty” part. The “dirty” part is the one communicating with public networks, e.g. ADSL, UMTS/3G, or LTE/4G modems. These components partly come from third party manufacturers in Taiwan, China, Korea, and the US. We do not trust these parts in our design;

they are treated like the unencrypted Internet, and are only used to establish an encrypted connection via them. The “clean” part of our products is completely under our control. The “dirty” part is separated from the “clean” part on the hardware but also on the software level.

4) Secure encryption, unbroken by the NSA

For encryption, all Viprinet VPN products use known industrial standards which are regarded as safe and unharmed by the NSA by security researchers.

These are in detail:

- TLS 1.1
- RSA, key length 1024 Bit until 8/2013, since then 2048 Bit
- AES 256 Bit
- SHA-1

Due to Edward Snowden's disclosures, it has to be assumed that the NSA may be trying to compromise widely common encryption libraries like OpenSSL or hardware encryption chips. US manufacturers are suspected to provide the VPN protocol IPSec of their devices with backdoors.

It has to be stated clearly: Viprinet doesn't use any unverified encryption engines of third parties. Our routers sure are equipped with hardware encryption engines; however, these originate from different manufacturers of different regions in the world, and are never used exclusively - we only use them in combination with encryption systems we've implemented in our software ourselves. Thus, our products are invulnerable for any of NSA's attack scenarios known so far, especially for weak random number generators.

Another advantage of Viprinet bonding technology is the fact that in our bonded VPN, only a fraction of the encrypted data is transmitted over a single Internet medium. Attack scenarios in the networks of network providers which have been conducted according to news accounts fail when used against our technology.

5) Actual risk areas

For bonding, Viprinet products use a centralized VPN hub in a data center. At this place, all encrypted data streams are combined. Attacking the encryption of our products will most likely happen in the data center's network. Thus, attention should be paid to whether the data center is certified in regards to security. Especially the VPN hub and neighboring network devices (e.g. switches) have to be protected against physical access.

Basically, man-in-the-middle attacks can occur with VPN technology implemented by Viprinet if password data of Viprinet routers is stolen via other gateways (e.g. social engineering, infiltrating spies, infecting administrator PCs). In future firmware releases, Viprinet will especially focus on these risks in order to distinctly improve security against and detectability of man-in-the-middle attacks.