SINA Box

The SINA Box can only be compared to conventional IPsec-based VPN gateways with regard to its functions. Due to the fact that the SINA Box is designed to serve as a high-security solution, these VPN functions are embedded into a specifically minimised and hardened Linux operating system and extended by particular, security-related additional functions. The SINA platform was developed by order of the German Federal Office for Information Security (BSI) which continuously analyses and evaluates the SINA components thoroughly.

About SINA Box

The SINA Box is an IPsec VPN gateway which connects secured or classified networks and protects them against attacks and manipulations. There are good arguments in favour of SINA technology:

- By means of SINA, different locations with networks requiring special protection can be connected in a highly secure and at the same time cost-efficient way via potentially insecure networks (e. g. the Internet).
- Up to now SINA is the only IP-based solution which was approved by the BSI for the transmission of information classified as VS-NfD, VS-Vertraulich, Geheim and Streng Geheim. Classified information and data networks of all national security gradings can also be protected in accordance with the German secret-protection guidelines.
- The SINA Technology holds a approval by BSI for the information network of the German federal administration (IVBV) and the information network Berlin – Bonn (IVBB).
- The German Federal Network Agency has approved SINA for surveillance measures according to the German Banking Act (KWG24) and the Telecommunications Surveillance Regulation (TKÜV).

The technology

The communication between SINA systems is strictly based on the security principle of a virtual private network (VPN). Due to the fact that the SINA Box is designed to serve as a high-security solution, these VPN functions are embedded into a specifically minimised and hardened Linux operating system (SINA Linux) and extended by particular, security-related additional functions. The cryptographic methods integrated into SINA comply with the current IPSec standard and can be selected freely by the user.

The software is provided on a tamper-protected CD-ROM or flash storage and is checked for integrity in connection with a smart card before it is started.

All initial configuration data and security relations of a SINA Box are stored in a specially protected area on a smart card. When the SINA Box is started, the security relations between all SINA Boxes of the respective network are established as IPsec VPN tunnels and, if necessary, additional security relations or configuration data are loaded from the SINA Management Server.

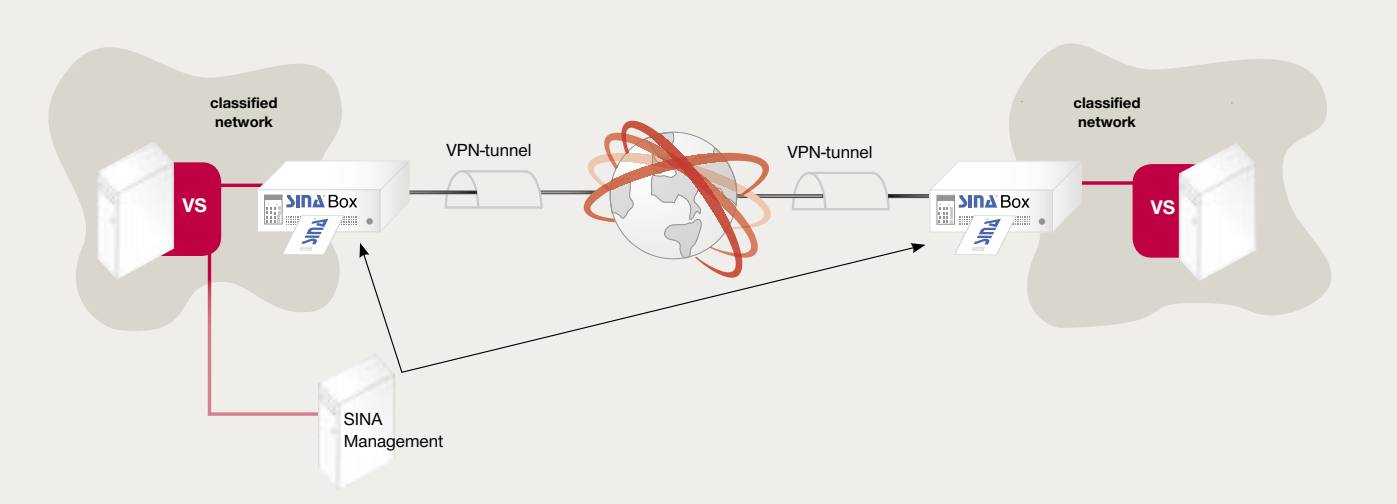
The configuration of all SINA Boxes within the network is executed by the SINA Management which is based on a public key infrastructure and uses a key management conforming to IPsec (IKE).

In addition, SINA Boxes can be monitored by means of logging mechanisms and intrusion detection & response systems.

Approvals

The SINA Box was intensively analysed and evaluated by the German Federal Office for Information Security and approved for the transmission of data of all national security classifications (VS-NfD, VS-Vertraulich, Geheim and Streng Geheim).

Moreover, the national use of SINA for the transmission of information up to the classification SECRET is approved by NATO.



Security features

For the processing and transmission of classified information with a higher security grading (> VS-NfD) the SINA Box is used in combination with radiation-proof (zoned) or manipulation-proof (tamper-protected) PC hardware. Over and above, differently strong cryptographic methods (hardware- and software-based) can be applied depending on the respective security classification.

Availability and services

The availability, performance and failure-safety of the SINA Box can be increased by means of load-balancing or a scalable cluster solution. The SINA Cluster consists of a group of SINA Boxes among which the data packets which are to be transmitted are distributed. Possible failures of a SINA Box will not be noticed by the user, since all affected connections will be taken over by the other SINA Boxes belonging to the cluster.

When a SINA Box is operated as hot-standby solution an automatic failover makes sure that the function of this broken-down SINA Box is taken over by the second SINA Box.

Moreover, the operational safety can be secured by means of an adequate service-level agreement (SLA) guaranteeing the recovery of defective hardware (not later than four hours within Germany).

SINA hardware

The security classification of the processed data is decisive for the type of hardware to be used: Depending on the required protection class and the corresponding approvals, the SINA technology either uses cost-efficient standard PC hardware or different types of tamper-protected or zoned special hardware. The requirements result from the specifications defined in the BSI approvals.

Sources of supply

German public authorities can purchase SINA technology according to the framework agreement BA 4867/01 of the procurement office of the Federal Ministry of the Interior.

Private enterprises and all foreign customers can procure SINA directly from secunet or the SINA resellers.

More than just security
secunet Security Networks AG is among the leading European service providers and product suppliers in the area of highly complex IT security solutions. More than 200 highly qualified employees with many years of experience develop intelligent and innovative solutions which generate sustainable added value for our customers. With our focus on top security in information technology, we are market leaders in Germany. Our reference list includes the majority of DAX30 companies and key international addresses as well as organisations and public authorities, at home and abroad. We offer our customers a complete range of services from consulting and development all the way to integration, training and service, and this from a single source. In doing so, secunet covers not only the traditional competence areas of security consulting and management, but also network and application security as well as the future fields of digital identity and signature and SINA® (Secure Inter-Network Architecture).

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen
Germany
Tel.: +49-201-5454-0
Fax: +49-201-5454-123

E-mail: sina@secunet.com
www.secunet.com