

## VPN-Gateway für vertrauliche Kommunikation



### Ihre Vorteile:

- » Zugelassen bis einschließlich VS-VERTRAULICH, NATO CONFIDENTIAL und CONFIDENTIEL UE
- » Hoher Datendurchsatz bis ca. 1 GBit/s
- » Hochverfügbar
- » Einfache Software-Updates
- » Etabliert in komplexen Sicherheitsnetzen

Die SINA Box ist als VPN-Gateway eine zentrale IT-infrastrukturelle Kernkomponente in VS-Netzwerken. Die zwischen den SINA Komponenten ausgetauschten Daten werden in kryptographischen VPN-Tunneln sicher übertragen. **Die SINA Boxen verbinden Behörden- oder Firmennetze über öffentliche Leitungswege, beispielsweise über das Internet.** Darüber hinaus laufen die Zugriffe von SINA Clients auf (Terminal-) Serverbereiche über vorgeschaltete SINA Boxen als kryptographische Netzzugangspunkte.

Die SINA Box S ist das einzige vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-VERTRAULICH zugelassene IPSec basierte VPN-Gateway mit softwarebasierter Kryptographie.

Die SINA Box S ist eine seit vielen Jahren anerkannte Standardlösung und wird u. a. in nationalen und internationalen behördlichen Sicherheitsnetzen eingesetzt. Diese Komponente schützt seit vielen Jahren komplexe nationale und internationale Behörden- und Firmennetze wie beispielsweise das Auswärtige Amt, das Führungsinformationssystem der Luftwaffe oder die Europäische Union.

Der Einsatz von SINA Boxen erfordert IP-fähige Transportnetze. Dies beinhaltet auch Satellitenkommunikationsstrecken. In Verbindung mit

Sat-Optimierern wird die verfügbare Bandbreite der Satellitenstrecken effektiv ausgenutzt.

#### IT-Sicherheitskonzept

Der SINA Box S liegt ein ganzheitliches IT-Sicherheitskonzept zugrunde. Dieses umfasst insbesondere

- eine gehärtete und evaluierte Linux-Systemplattform,
- Smartcard-Technologie,
- IPSec-basierte Kryptographie sowie
- zulassungskonform dimensionierte und konfigurierte Hardware, Firmware und Software.

Kryptographische Schlüssel, Konfigurationsdaten und Sicherheitsbeziehungen sind durch eine Smartcard geschützt.

**Sicherer Systemstart und Betrieb**

Unter Berücksichtigung der konkreten IT-infrastrukturellen Gegebenheiten und projektspezifischer kommunikativer Anforderungen sind die SINA Boxen S mit bis zu mehreren tausend Sicherheitsbeziehungen einsetzbar.

Die SINA Box Software wird (in der VS-VERTRAULICH-Konfiguration) vertrauenswürdig von CD-ROM beim Systemstart geladen. Alle initialen Konfigurationsdaten und Sicherheitsbeziehungen der SINA Box werden in einem geschützten Bereich der SINA Smartcard gespeichert. Beim Starten der SINA Box werden die Sicherheitsbeziehungen zum SINA Management und den kommunikationsrelevanten SINA Boxen als IPSec-VPN-Tunnel aufgebaut. Falls notwendig, werden zusätzliche Sicherheitsbeziehungen oder Konfigurationsdaten vom SINA Management geladen. Das macht die SINA Box sehr einfach in ihrer Konfiguration, Installation, beim Roll-Out und beim Austausch von Hardware.

Im Betrieb protokollieren die SINA Boxen überwachungsrelevante Daten. Diese können in Netzwerkmanagementsysteme importiert und dort bedarfsgerecht aufbereitet bzw. visualisiert werden.

**Hochverfügbarkeit**

Die Verfügbarkeit und Ausfallsicherheit von SINA Boxen kann mittels redundanter Konfigurationen erhöht werden. Dabei wird durch automatisches Umschalten die Funktion der ausgefallenen SINA Box (Master) durch eine zweite SINA Box (Slave) übernommen.

**Management**

Die Konfiguration aller SINA Boxen im Netzwerk erfolgt zentral durch das SINA Management. Eine integrierte Public-Key-Infrastruktur (PKI) mit zugehörigem Benutzermanagement unterstützt wesentliche administrative Prozesse rund um die SINA Smartcards, insbesondere deren Personalisierung, die Generierung bzw. Aktualisierung von Schlüsseln und kryptographischen Parametern sowie die Verwaltung der zugehörigen PINs und PUKs.

**Bezugsquellen**

Behördenkunden in Deutschland können die SINA Komponenten aus dem Rahmenvertrag BA 4867/01 des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Allen anderen nationalen und internationalen Kunden stehen secunet bzw. autorisierte Vertragspartner gern zur Verfügung.

**Modellvarianten**

	SINA Box LE	SINA Box 1HE (5LAN)	SINA Box 1000	SINA Box 3HE Zone 1
				
Symmetrische Kryptoverfahren	AES	AES	AES	AES
Asymmetrische Kryptoverfahren	EC-GDSA, EC-DH	EC-GDSA, EC-DH	EC-GDSA, EC-DH	EC-GDSA, EC-DH
Kryptodatendurchsatz	ca. 10 MBit/s	ca. 90 MBit/s	ca. 900 MBit/s	ca. 90 MBit/s
Netzwerkschnittstellen	3 x 10/100 MBit Cu	5 x 10/100 MBit Cu	5 x 10/100/1000 MBit Cu	4 x 100 MBit LWL oder 4 x GBit LWL oder je 2 x 100 MBit und 1 GBit LWL
Abstrahlenschutz	—	—	—	Zone 1
Zulassungen	 VS-NfD	VS-NfD	VS-NfD	VS-VERTRAULICH
	 NATO RESTRICTED	NATO RESTRICTED	NATO RESTRICTED	NATO CONFIDENTIAL
	 RESTREINT UE	RESTREINT UE	RESTREINT UE	CONFIDENTIEL UE

**Über SINA**

Im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelte secunet die Sichere Inter-Netzwerk Architektur SINA. Die Kryptosystem-Produktfamilie ermöglicht eine bedarfsgerechte, zulassungskonforme sichere Bearbeitung, Speicherung und Übertragung von Verschlusssachen sowie anderen sensiblen Daten.

Das Produktportfolio umfasst ein Management, unterschiedliche Gateways, Leitungsverschlüssler und Clients, die seit vielen Jahren bereits bei Behörden, Streitkräften und geheimschutzbetreuten Unternehmen eingesetzt werden. Ausgewählte SINA Komponenten sind für die Verarbeitung und Übertragung von VS der Einstufungen bis einschließlich STRENG GEHEIM, NATO SECRET und SECRET UE zugelassen.

Weitere Informationen:  
[www.secunet.com/box](http://www.secunet.com/box)

**secunet**

secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen

Tel.: +49-201-5454-0  
Fax: +49-201-5454-1000  
E-Mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)