

# Gehärtetes VPN-Gateway

Für GEHEIM



# Die SINA L3 Box H R 200M-2 ist als VPN-Gateway eine zentrale IT-infrastrukturelle Kernkomponente in Hochsicherheitsnetzwerken.

Die zwischen den SINA Komponenten ausgetauschten Daten werden in verschlüsselten VPN-Tunneln sicher übertragen. Die SINA L3 Boxen verbinden Behörden- oder Firmennetze über das Internet. Darüber hinaus werden die Zugriffe von SINA Clients auf (Terminal-)Serverbereiche auf vorgeschalteten SINA L3 Boxen kryptographisch terminiert.

Mit der SINA CORE basierten SINA L3 Box H R 200M-2 wurde ein IP-Verschlüsselungsgerät für nationale und internationale Netze entwickelt, welches vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Übertragung von Verschlusssachen für GEHEIM bis STRENG GEHEIM zugelassen ist. Im Fokus stehen dabei militärische und Hochsicherheitsnetze.

Gegenüber dem Vorgängermodell SINA L3 Box H R 200M ist die SINA L3 Box H R 200M-2 deutlich performanter, kompakter und leichter. Mit 200 MBit/s Vollduplex wird der Datenverschlüsselungsdurchsatz mehr als verdoppelt. Die Bauform der Hardwareplattform wurde mit 1 ½ Höheneinheiten und 19/2" ganz erheblich verringert. Die Benutzerfreundlichkeit wurde durch eine langlebige Batterie erhöht. Die Hardwareplattform verfügt über nur noch einen, nunmehr siegelgesicherten Notlöschstaster. Vorsätzliche und Fehlbetätigungen sind damit äußerlich einfacher erkennbar. Die SINA L3 Box H R 200M-2 ist in vielerlei Hinsicht flexibel einsetzbar, u. a. durch nachladbare Krypto-Geräteklassen, erweiterte Temperaturbereiche, direkt am Gerät

umkonfigurierbare Netzwerkschnittstellen sowie eine moderate Leistungsaufnahme. Darüber hinaus werden mit der neuen Softwareversion neben IPv6, IKEv2, SHA-256 und VLAN auch diverse Remote-Funktionalitäten unterstützt. Diese umfassen Updates der SINA Software, der Smartcard-Konfiguration und der operativen Parameter der SINA CORE Module. Außerdem sind Remote-Zugriffe auf die Administrator-Schnittstelle möglich.

## IT-Sicherheitskonzept

Der SINA L3 Box H R 200M-2 liegt ein ganzheitliches IT-Sicherheitskonzept zugrunde. Dieses umfasst insbesondere:

- eine gehärtete und intensiv evaluierte SINA OS-Systemplattform
- Smartcard-Technologie
- IPsec-basierte Kryptographie
- ein SINA CORE Kryptomodul
- zulassungskonform dimensionierte und konfigurierte Hardware, Firmware und Software.

## Sicherer Systemstart und Betrieb

Die SINA L3 Box Software wird coreboot gesichert vertrauenswürdig beim Systemstart vom Flash-Speicher geladen. Alle initialen Konfigurationsdaten und Sicherheitsbeziehungen der SINA L3 Box werden in einem geschützten Bereich der SINA Smartcard gespeichert. Beim Starten einer SINA L3 Box werden die Sicherheitsbeziehungen zum SINA Management und den primär kommunikationsrelevanten SINA L3 Boxen als IPsec-VPNTunnel aufgebaut. Falls notwendig, werden zusätzliche Sicherheitsbeziehungen oder Konfigurationsdaten vom SINA Management geladen. Das macht die SINA L3 Box sehr einfach in ihrer Konfiguration, Installation und beim Austausch von Hardware.

## Betriebsüberwachung

Im Betrieb protokollieren die SINA L3 Boxen überwachungsrelevante Daten. Diese können in Netzwerkmanagementsysteme importiert und dort bedarfsgerecht aufbereitet bzw. visualisiert werden. Darüber hinaus sind ausgewählte Daten über SNMP abfragbar.

## Einsatz unter rauen Umweltbedingungen

Die SINA L3 Box H R basiert auf einer gehärteten, unter rauerer Umweltbedingungen einsetzbaren Hardware-Plattform, die auszugswise die anspruchsvollen Anforderungen des MIL-STD-810G erfüllt. Die nach außen geführten Schnittstellen sind separat geschützt. Das Gehäuse bietet einen erhöhten Schutz insbesondere gegen Schock, Vibration, Staub und Feuchtigkeit. Darüber hinaus kann die SINA L3 Box H R 200M-2 gegenüber dem Vorgängermodell in einem erweiterten Temperaturbereich betrieben werden.

## Hochverfügbarkeit

Die Verfügbarkeit und Ausfallsicherheit von SINA L3 Boxen kann mittels redundanter Konfigurationen erhöht werden. Dabei wird beispielsweise durch automatisches Umschalten die Funktion der ausgefallenen, bislang aktiven SINA L3 Box durch eine zweite SINA L3 Box (hot standby) übernommen. Ab der Softwareversion 3.10 sind die Umschaltzeiten deutlich kürzer.

Darüber hinaus unterstützen SINA L3 Boxen auch auch georedundante und lastverteilende Konfigurationen. Bei georedundanten Szenarien laufen die alternativen, bedarfsgerecht priorisierbaren Kommunikationswege über – an unterschiedlichen Standorten befindliche – SINA L3 Boxen. Bei Lastverteilungskonfigurationen interagieren die SINA L3 Boxen mit handelsüblichen Loadbalancern.

## Satellitenkommunikation

Der Einsatz von SINA L3 Boxen erfordert IP-fähige Transportnetze in klu sive Satellitenkommunikationsstrecken. In Verbindung mit Sat-Optimierern wird die verfügbare Bandbreite der Satellitenstrecken effektiv ausgenutzt.

## Vorteile

- Zugelassen für GEHEIM
- Remote-Funktionalitäten
- Höhere Performance
- Robuste Hardwareplattform
- Kompakte Bauform
- Umschaltbare Netzwerkschnittstellen
- Komfortables Management



## Management

Die Konfiguration aller SINA L3 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 Smartcards der SINA L3 Boxen. Dazu gehören insbesondere deren Personalisierung, die Generierung bzw. Aktualisierung von Schlüsseln und kryptographischen Parametern sowie die Verwaltung der zugehörigen PINs und PUKs.

## Zulassungsrelevante Konstruktionsstände



### SINA L3 Box H R 200M-2 27A

Leistungsdaten	
Zulassungsgrad	GEHEIM, STRENG GEHEIM*
Boot-Integritätsschutz	coreboot
Softwareversion	3.10
Manipulationsschutz	integriert
Abstrahlschutz	SDIP 27 Level A
Authentifizierungstoken	SINA Smartcard

## Technische Daten

Allgemeine Daten	
Abmessungen (B × H × T)	210 × 65 × 350 mm
Gewicht	10 kg (ohne Montageplatte)
Leistungsaufnahme	45 W
Spannungsversorgung	DC 24 V (24 ... 28 V) / 3 A
BTU/h	153,4
Kryptohardware	
Modul	SINA CORE 2 L3
Verschlüsselungsleistung	200 MBit/s
Symmetrische Kryptoverfahren	Libelle, VEGAS
Asymmetrische Kryptoverfahren	EC-GDSA, EC-DH
LAN-Anschlüsse	
Netzwerkschnittstellen	1 × 100/1000 MBit LWL (umschaltbar) 1 × 100/1000 MBit LWL in SINA CORE (umschaltbar)
Steckertyp	LC
Temperaturbereiche	
Betrieb	-15 °C bis +45 °C
Transport und Lagerung	-25 °C bis +60 °C
Sonstiges	
Schutzart	IP67
Härtung	MIL-STD-810G

\*Bei Einsatzfällen, in denen Daten der Einstufung STRENG GEHEIM verarbeitet werden, ist das Einsatzszenario und das IT-Sicherheitskonzept für die SINA L3 Box H R 200M-2 gesondert mit dem BSI abzustimmen.

### Bezugsquellen

Behördenkunden in Deutschland können die SINA L3 Box H R 200M-2 aus dem Rahmenvertrag 5070 „Kryptiergeräte der SINA Familie“ des Beschaffungsamtes des Bundesministeriums des Innern oder über den SINA Ergänzungsvertrag Q/IB1C/R6359 der Bundeswehr beziehen. Allen anderen nationalen und internationalen Kunden steht secunet gern zur Verfügung.

### secunet Security Networks AG

Kurfürstenstraße 58 · 45138 Essen

T +49 201 5454-0 · F +49 201 5454-1000

info@secunet.com · secunet.com

Weitere Informationen:  
[secunet.com/sina](https://www.secunet.com/sina)

**secunet**