The new SINA L2 Box S 100G

Since August 2020, the SINA L2 Box S product portfolio has been expanded by a new high-performance hardware version. With an impressive encryption performance of up to 100 Gbit/s and an encryption level to VS-NfD (Restricted), the new SINA L2 Box S 100G is now available and offers numerous new application opportunities.

In the course of advancing digitisation and the associated automation, there is an ever-increasing demand for IT services, which puts additional pressure on bandwidth requirements for the transmission of digital data. Especially in the context of data centres and cloud-based applications, requirements are rapidly rising to the range of 100 GBit/s. Commercially available layer 2 encryptors approved by the German Federal Office for Information Security (BSI) can often only provide this bandwidth by clustering multiple systems. This requires increased space and energy. The new SINA L2 Box S 100G can be used efficiently in various scenarios due to its extremely high encryption performance.

What is SINA?

SINA (secure inter-network architecture) provides an entire ecosystem for approval-compliant data communication. From the SINA Workstation as a user endpoint, to the SINA L2 Box and the SINA L3 Box for layer 2 and 3 network encryption, up to SINA Management.

Interconnection of data centres by means of fibre-optic cables

The SINA L2 Box S 100G allows to establish encrypted layer 2 point-to-point connections, which are VS-NfD (Restricted) compliant, between two or even multiple data centres (ring topologies). Through these connections applications within the data centres can communicate securely between the data centres on layer 2 and 3.

This creates a broad range of applications for the new SINA L2 Box S 100G, the interconnection of data centres via fibre-optic cables or WDM connections. Both the connection infrastructure and the available space in the data centre can be used much more efficiently due to the higher bandwidth of a single box. Furthermore, this is of great importance for data centres with high availability requirements.

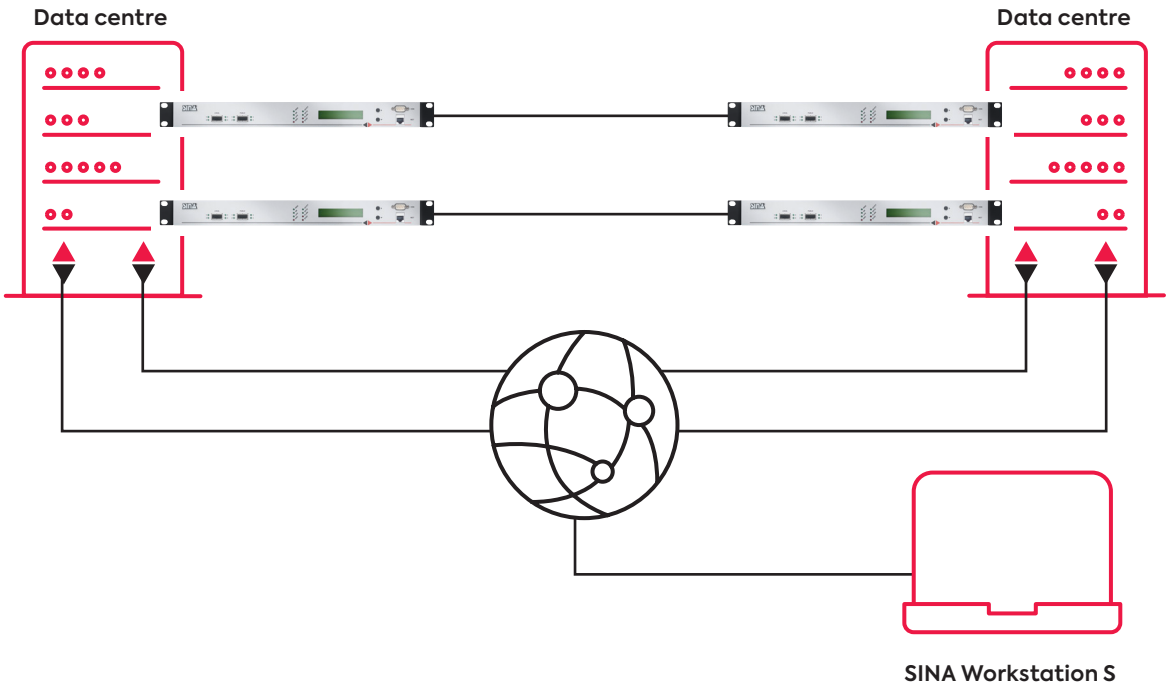

Figure 1: Data centre with redundant interconnection using SINA L2 Box S

The SINA L2 Box S 100G thereby provides a highly secure firewall function at the access point to the data centre because it only allows cryptographically authenticated packets to pass through while immediately dropping any invalid packets hardware-based at line rate.

This was previously limited to a maximum data rate of 40 GBit/s but is now also available for up to 100 GBit/s. Licence options (50 GBit/s) allow the SINA L2 Box S 100G to be adapted to initially lower bandwidth requirements. If, at a later stage, bandwidth demand increases only a license upgrade is needed instead of replacing hardware.

WDM system

Another important application is the encryption of data to be transmitted via WDM[1] connections. In many cases, the entire data stream between the terminals is encrypted (layer 1 encryption). However, this is currently only certified in a few cases for VS-NfD (Restricted) and does not allow the separation of responsibility for data transmission and cryptography. Especially in larger organisations, different responsibilities for network technology and cryptography exist. If both functions are integrated into one system, the responsibility for operation and configuration cannot be clearly assigned. Furthermore, in most cases the transfer at the interfaces of the WDM systems is done in layer 2- Ethernet format anyway.

SINA L2 Box S 100G now enables the encryption of a complete 100GBit/s wavelength connection on layer 2 without affecting the network topology.
The responsibility for cryptography and data transport can be separated according to requirements, and both encrypted and unencrypted wavelengths can be transmitted together.

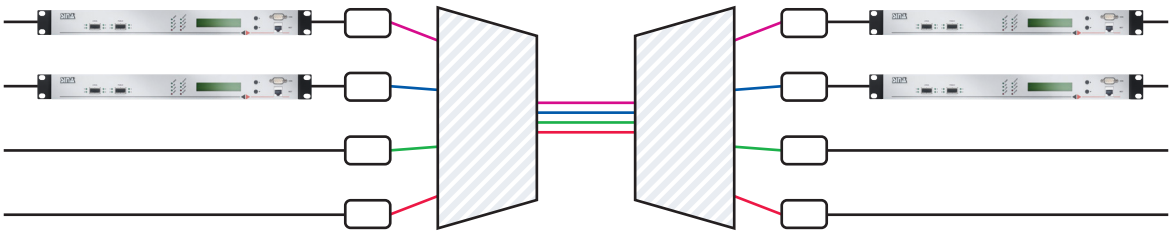

Figure 2: SINA L2 Box S in combination with WDM systems

1 WDM = Wavelength Division Multiplex

Site-to-site networking

In addition to the interconnection of data centres and WDM application scenarios, the significantly higher bandwidth of the SINA L2 Box S 100G also results in advantages for layer 2 site-to-site networking. With star-shaped topologies in particular, considerably higher bandwidth requirements can arise at the main sites.

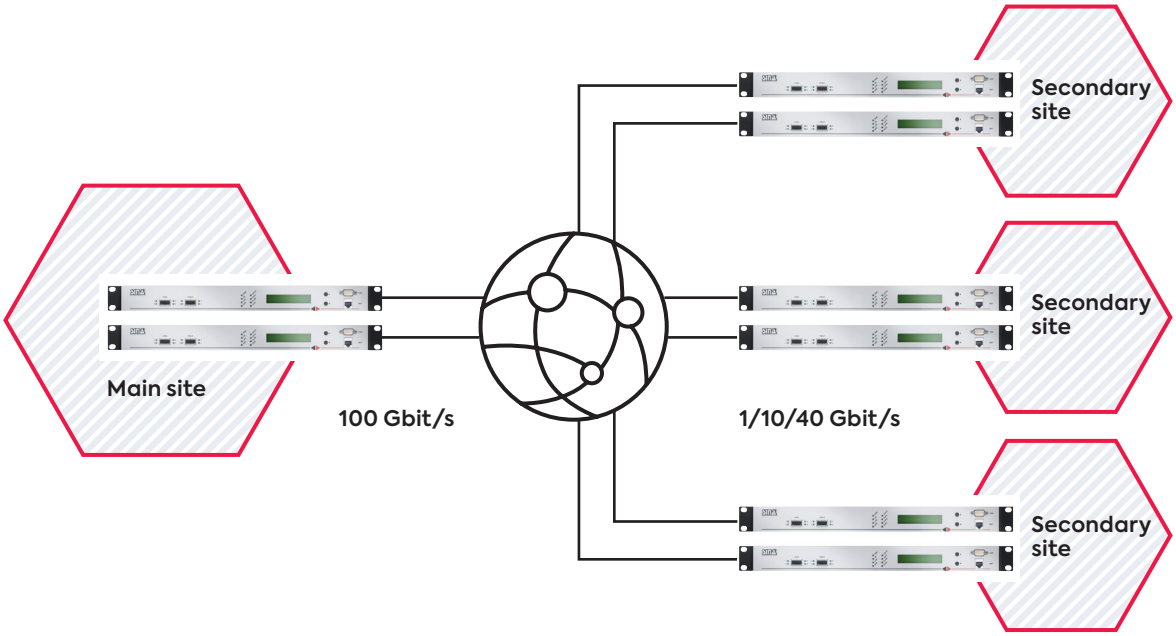

Figure 3: SINA L2 Box S in the context of site-to-site networking (the drawing shows redundant interconnects in order to avoid any single points of failure)

A more powerful SINA L2 Box S can be integrated instead of clustering multiple systems. As with the interconnection of the data centre, both the connection infrastructure used (e.g. fibre-optics) and the available space in the network node locations can be used much more efficiently thanks to the now higher bandwidth capacity.

SD-WAN ready?

The SINA L2 Boxes S with their high encryption performance also provide attractive solutions for new application scenarios in the SD-WAN environment.

In contrast to classic IP address-based routing, SD-WAN (Software Defined – Wide Area Network) uses additional information and rules for packet forwarding. This is done by defining policies in which the requirements of the applications and the quality of the available networks can be taken into account.

SD-WAN topologies are categorised into overlay and underlay. The overlay is where the flow classification takes place and the policy-based forwarding decision is made. The underlay is where the data transport between sites takes place. Several underlay networks can be used in parallel. This allows for increased redundancy or cost optimisation through the partial use of Internet-based connections.

For example, the data packets from a VoIP application can be recognised through flow classification. These data packets can then be forwarded by a specific policy, e.g. “forwarding via the underlay network with the currently lowest delay”.

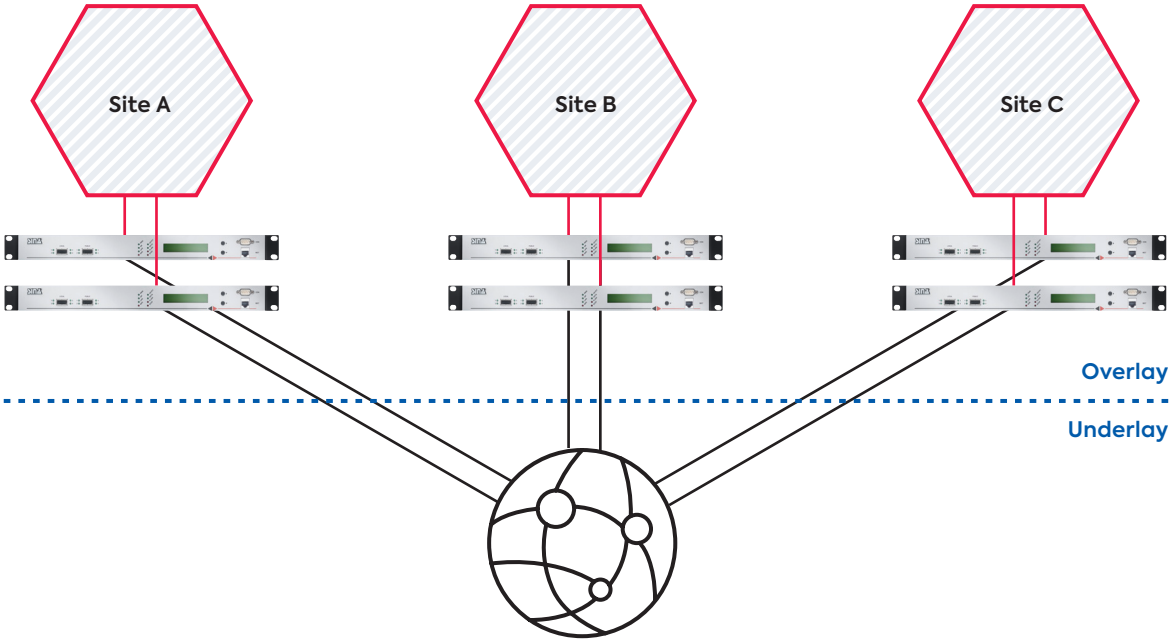

Figure 4: SINA L2 Box S in the context of SD-WAN (the drawing again shows redundant interconnects in order to avoid any single points of failure).

Since underlay networks are usually set up over infrastructures that are not trustworthy in terms of security, the data content needs to be encrypted on its way through the underlay. This has to happen at the edge between the overlay and the underlay.

A significant advantage gained from using layer 2 encryption technologies at the transition between the overlay and underlay is the transparency for layer 3. Instead of handling individual IP flows the whole packet stream between the sites is encrypted on layer 2 level. The SINA L2 Box S thus provides a transparent and independent encryption function without affecting the policy based forwarding functions provided by SD-WAN.

If mainly sites and data centres are interconnected, the number of endpoints is usually in the small to medium range. However, individual bandwidths can become very high sometimes. The SINA L2 Box S with its various performance levels from 10 Gbit/s to 40 Gbit/s and up to 100 Gbit/s is ideally suited for these application scenarios.

Thus network operators are free to choose the SD-WAN solution in the unencrypted overlay network section. Furthermore, when using the SINA L2 Box S, the user receives a transparent VS-NfD-approved solution for secure data exchange Made in Germany, regardless of the actual SD WAN manufacturer.

Post-quantum cryptography

The SINA L2 Box S also has something to offer in terms of post-quantum cryptography (PQC). This is because it already follows the recommendation of the German Federal Office for Information Security (BSI) for action on “migrating to post-quantum cryptography”.

The SINA L2 Box S uses a pre-distributed symmetric long-term key for regular key derivation, which is made available in the device via a PIN-protected smart card. This makes it possible to symmetrically encrypt the asymmetric key exchange between two devices using a distributed secret.

For cryptography on elliptical curves, the SINA L2 Box S also offers the option of keeping curve parameters secret. This minimises the attack vector against attacks with quantum computers, since the curve parameters can be calculated if three points on the curve are known.

Higher efficiency thanks to layer 2

In principle, it is possible to establish data connections on different layers of the OSI model. One speaks of layer 1 (L1) if the connection is established directly on the physical layer (e.g. as a bit stream in a WDM system). Layer 2 (L2) is used for Ethernet connections and layer 3 (L3) for IP connections.

Depending on the requirements of the application environment, layer 2 or layer 3 solutions have specific operational advantages. As a general guideline, a layer 3-based solution has scaling advantages for a high number of endpoints with low bandwidth requirements (e.g. VoIP endpoints or mobile access points) and aggregation at larger sites or mobile access points.

On the other hand, when it comes to larger endpoint bandwidths, more symmetrical topologies and a small to medium number of endpoints, layer 2-based solutions have an advantage in terms of data transmission and operation efficiency.

Layer 1-based solutions are currently primarily used for point-to-point connections (e.g. WDM connections), and provide the infrastructure for the higher transmission layers.

Similar considerations apply when selecting the encryption level. The main point of use for layer 2 encryption is with high connection bandwidths (> 1 Gbit/s) and a small to medium number of endpoints (usually <100). A major advantage is the transport efficiency. With layer 2 encryption, less overhead is added over all and thus the available bandwidth is used more efficiently.

Furthermore, layer 2 connections also offer the advantage of operational efficiency. With layer 2 encryption, the IP layer remains unaffected and the end user remains in full control over IP-based forwarding of packets. As a result, there is no need to encrypt each IP connection individually, and consequently fewer security relationships need to be considered. In addition to this, it is possible to use other routing or forwarding technologies (SDN/SD-WAN) at any time, regardless of the encryption solution chosen.

For further information on secunet's products for secure layer 2 and layer 3 data exchange, please visit: **www.secunet.com/sina**