Die neue SINA L2 Box S 100G

Seit August 2020 ist das Produktportfolio der SINA L2 Box S um eine neue leistungsfähige Hardware-Version gewachsen. Mit einer imposanten Verschlüsselungsleistung von bis zu 100 Gbit/s ist die neue, im Verschlussgrad VS-NfD zugelassene SINA L2 Box S 100G, nun verfügbar und bietet eine Vielzahl neuer Einsatzmöglichkeiten.

Im Zuge fortschreitender Digitalisierung und damit einhergehender Automatisierung nimmt der Bedarf für IT-Dienstleitungen und somit ebenfalls der Bandbreitenbedarf bei der digitalen Datenübertragung stetig zu. Gerade im Umfeld von Rechenzentren und cloudbasierten Anwendungen steigen die Anforderungen schnell in den Bereich von bis zu 100 Gbit/s. Marktübliche, durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Layer2-Verschlüsseler, können diese Bandbreiten oft nur über mehrere parallel eingesetzte Systeme abdecken. Dies erfordert einen erhöhten Platz- und Energiebedarf. Die neue SINA L2 Box S 100G kann durch die sehr hohe Verschlüsselungsleistung effizient in verschiedenen Szenarien eingesetzt werden.

Was ist SINA?

SINA (Sichere Inter-Netzwerk Architektur) stellt ein gesamtes Ökosystem für die zulassungskonforme Datenkommunikation bereit. Von der SINA Workstation als Client, über SINA L2 Box und SINA L3 Box für die Netzwerkverschlüsselung auf Layer 2 und 3, bis hin zum SINA Management.

Rechenzentrumskopplung über Glasfaserkabel

Mit der SINA L2 Box S 100G lassen sich sichere Layer2–Punkt-zu-Punkt VS-NfD-konforme-Tunnelverbindungen zwischen zwei oder auch mehren Rechenzentren (Ring Topologie) aufbauen, über die die Applikationen in und auch zwischen den Rechenzentren auf Layer2- und Layer3-Ebene abgesichert kommunizieren können.

Damit ergibt sich ein Haupteinsatzfeld für die neue SINA L2 Box S 100G: Die Kopplung von Rechenzentren über Glasfaserkabel oder WDM-Verbindungen. Hierbei kann sowohl die eingesetzte Verbindungsinfrastruktur als auch der verfügbare Platz im Rechenzentrum durch die nun höheren verfügbaren Bandbreiten deutlich effizienter genutzt werden. Dies ist besonders im Umfeld von hochverfügbaren Rechenzentrums-Clustern von enormer Bedeutung.

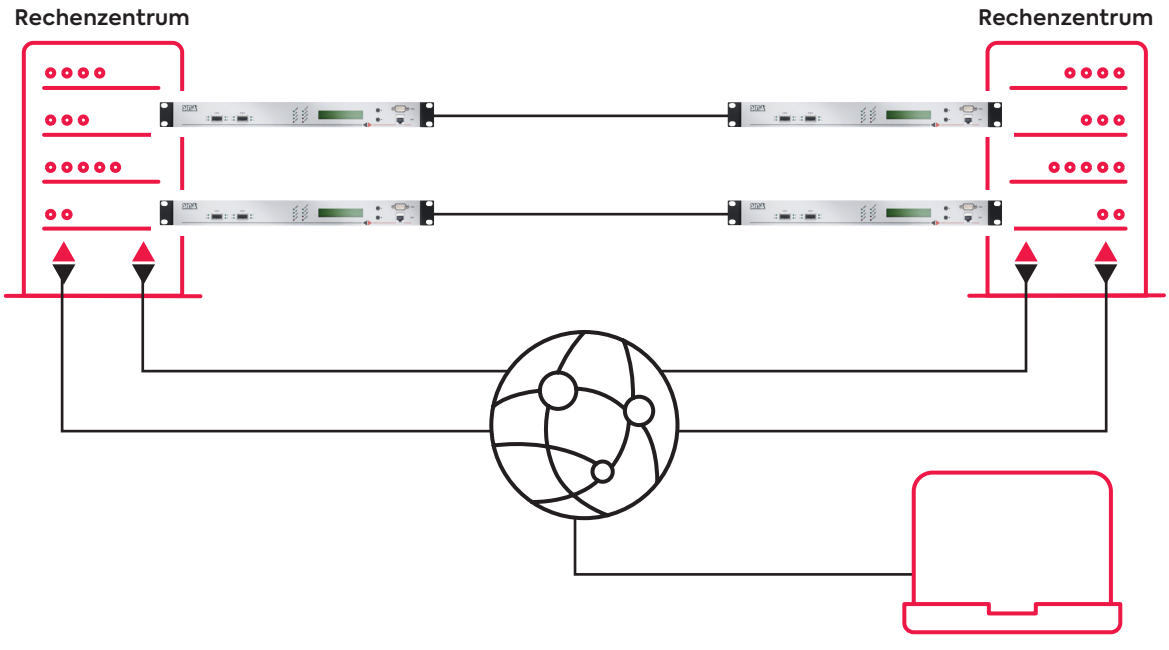

Abbildung 1: Rechenzentrumskopplung mit SINA L2 Box S

Die SINA L2 Box S 100G stellt dabei eine hochsichere Firewall-Funktion am Zugang zum Rechenzentrum dar, da nur kryptographisch authentifizierte Pakete durchgelassen und ungültige Pakete umgehend, hardwarebasiert verworfen werden.

Dies war bisher auf eine maximale Datenrate von 40 Gbit/s beschränkt und ist nun auch für bis zu 100 Gbit/s verfügbar. Durch Lizenzoptionen (50 Gbit/s) kann die SINA L2 Box S 100G an einen anfänglich niedrigeren Bandbreitenbedarf angepasst werden. Später, im Laufe des Lebenszyklus, lässt sich nur durch Lizenzupgrade die Leistung steigern, um einem steigenden Bedarf gerecht zu werden.

WDM System

Ein weiteres wichtiges Einsatzfeld ist die Verschlüsselung von Daten, die über WDM[1]-Verbindungen übertragen werden sollen. In vielen Fällen wird hier auf die Verschlüsselung des gesamten Datenstroms zwischen den Endstellen gesetzt (Layer1-Verschlüsselung). Dies ist aber derzeit nur in wenigen Fällen für VS-NfD zertifiziert und erlaubt keine Trennung der Verantwortung für die Datenübertragung und die Kryptographie. Denn gerade bei größeren Organisationen gibt es unterschiedliche Verantwortlichkeiten für die Netzwerktechnik und die Kryptographie. Sollten beide Funktionen in einem System verbaut sein, ist die Zuständigkeit für den Betrieb und die Konfiguration nicht eindeutig zuordenbar. Hinzu kommt, dass in den allermeisten Fällen die Übergabe an den Schnittstellen der WDM Systeme ohnehin im Layer2-Ethernet-Format erfolgt.

Mit der SINA L2 Box S 100G wird es nun möglich komplette 100Gbit/s Wellenlängen-Verbindung auf der Layer2 zu verschlüsseln, ohne dass sich das in der Netzwerk-Topologie bemerkbar macht. Die Verantwortung für Kryptographie und Datentransport kann damit anforderungsgerecht getrennt, sowie verschlüsselte und unverschlüsselten Wellenlängen gemeinsam übertragen werden.

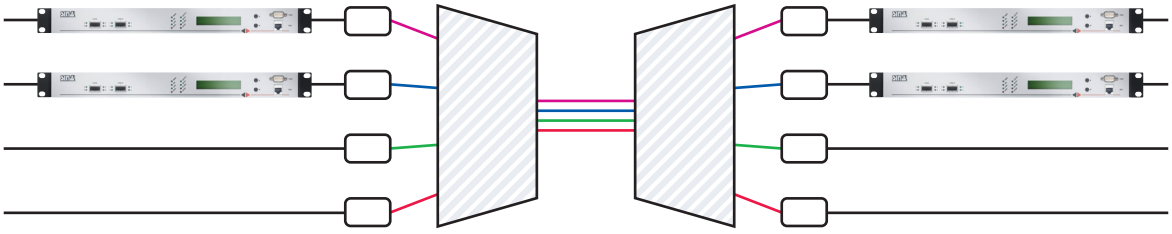

Abbildung 2: SINA L2 Box S in Verbindung mit WDM-Systemen

1 WDM = Wavelength Division Multiplex

Standortvernetzung mit Hauptstandort

Neben Rechenzentrumskopplung und WDM-Einsatzszenarien ergeben sich auch Vorteile bei der Layer2 Standortvernetzung durch die deutlich höhere Bandbreite der SINA L2 Box 100G. Gerade bei sternförmigen Topologien entstehen an den Hauptstandorten erheblich höhere Bandbreitenbedarfe.

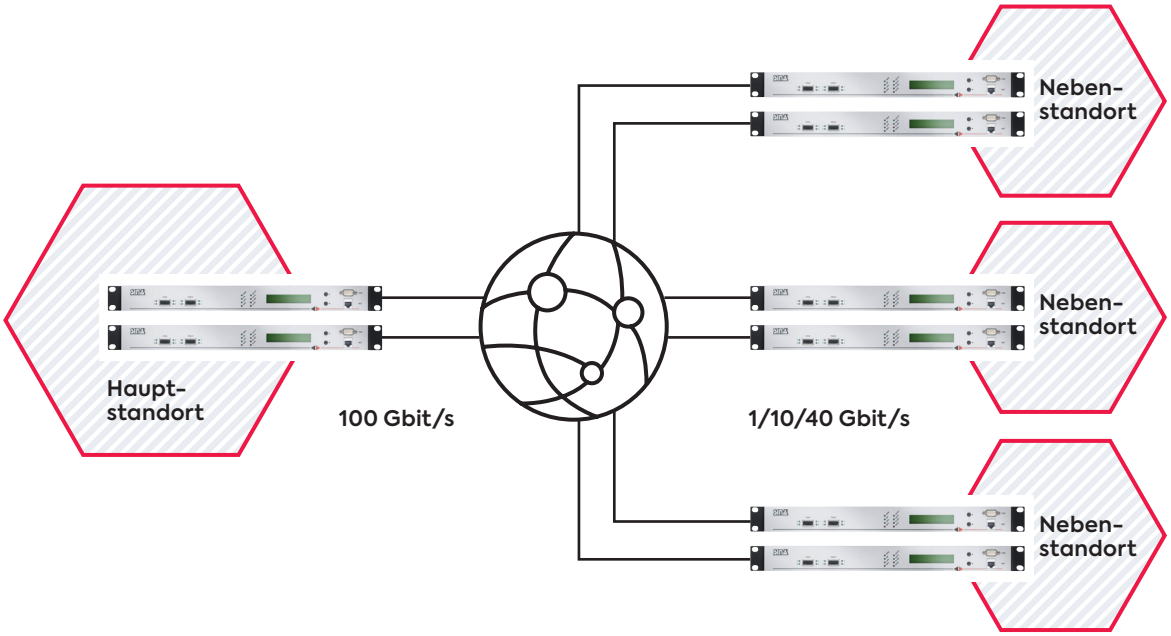

Abbildung 3: SINA L2 Box S im Kontext Standortvernetzung (zweifache Implementierung skizziert zur Vermeidung eines Single Point of Failure)

Statt mehrere parallele Übergänge einzusetzen, kann eine leistungsfähigere SINA L2 Box S integriert werden. Eine Dopplung ist nur noch aus Redundanzgründen erforderlich. Dadurch kann sowohl, wie bei der Rechenzentrumskopplung, die eingesetzte Verbindungsinfrastruktur (z.B. Glasfaser), als auch der verfügbare Platz in den Netzknotenstandorten durch die nun höheren verfügbaren Bandbreiten deutlich effizienter genutzt werden.

SD-WAN ready?

Doch auch für neue Anwendungsszenarien im SD-WAN-Umfeld liefern die SINA L2 Boxen S mit hohen Verschlüsselungsleistungen attraktive Lösungen.

Im Unterschied zum klassischen IP-adressbasierten Routing werden bei SD-WAN (software defined-wide area network) zusätzliche Informationen zur Paketweiterleitung verarbeitet. Dies passiert durch das Aufstellen von Regelwerken, bei denen u.a. die Anforderungen der eingesetzten Applikationen und die Qualität der verwendeten Netzwerke mitberücksichtigt werden können.

Bei SD-WAN Topologien unterscheidet man zwischen Overlay und Underlay. Im Overlay findet die Verkehrsklassifizierung (flow classification) statt und es erfolgt die regelbasierte Weiterleitungsentscheidung (policy based forwarding). Im Underlay findet der Datentransport zwischen den Standorten statt. Dabei können auch mehrere Underlay-Netzwerke zum Einsatz kommen. Hierdurch erreicht man eine Redundanzerhöhung oder eine Kostenoptimierung durch die teilweise Nutzung von Internet-basierten Verbindungen.

Beispielsweise können die Datenpakete aus einer VoIP-Applikation entsprechend erkannt werden (flow classification). Im Folgenden können diese Datenpakete über eine entsprechende Regel, z.B. „Weiterleitung über das Underlay-Netz mit der aktuell niedrigsten Laufzeit“ regelkonform und effizient transportiert werden (policy based forwarding).

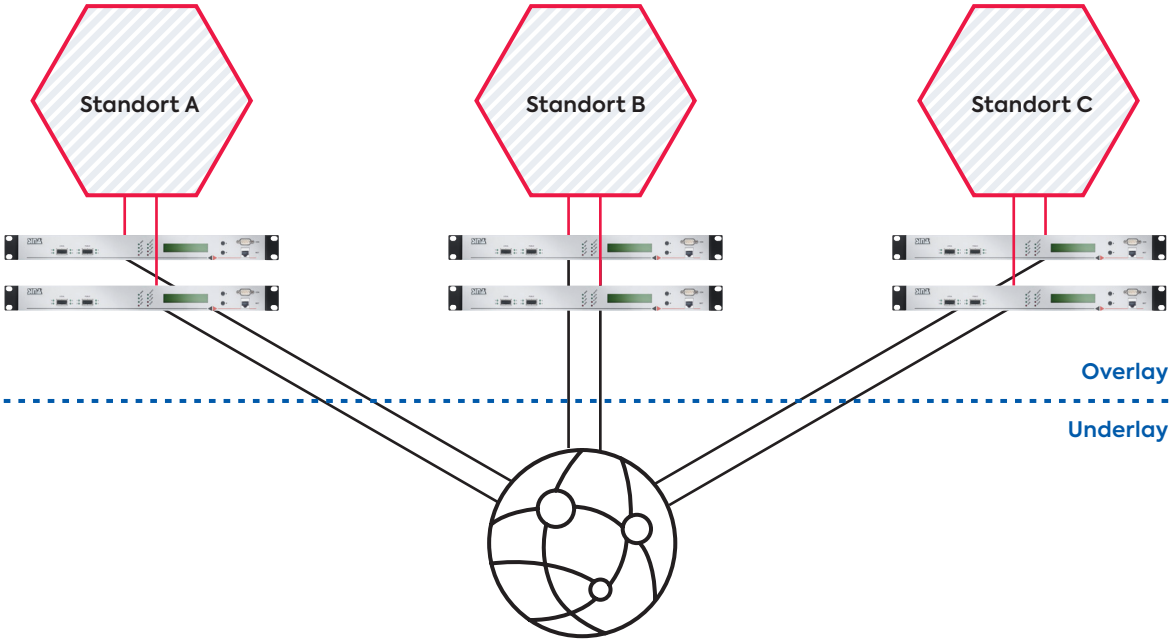

Abbildung 4: SINA L2 Box S im Kontext von SD-WAN

Da die Underlay-Netzwerke meist über sicherheitstechnisch nicht vertrauenswürdige Infrastrukturen aufgespannt werden, müssen spätestens am Übergang zwischen Overlay und Underlay die Dateninhalte verschlüsselt werden.

Ein wesentlicher Vorteil des Einsatzes der Layer2 Verschlüsselungstechnologien am Übergang zwischen Overlay und Underlay ist die Transparenz für Layer3 Weiterleitungsentscheidungen. Statt individuelle IP-Verbindungen zu behandeln, wird jeweils nur der entsprechende Datentransport zwischen den Standortübergängen (Overlay-Underlay-Übergang) auf der Layer2-Ebene bearbeitet. Die SINA L2 Box S stellt somit eine transparente und unabhängige Verschlüsselungsfunktion bereit, ohne die vom SD-WAN bereitgestellte Netzwerkfunktionen zu beeinflussen.

Werden im wesentlichen Standorte und Rechenzentren miteinander verbunden, so ist die Anzahl der Endpunkte meist im kleinen bis mittleren Bereich. Die individuellen Bandbreiten können aber zum Teil sehr hoch werden. Für dieses Anwendungsszenario eignet sich die SINA L2 Box S in ihren verschiedenen Leistungsstufen von 10 Gbit/s über 40 Gbit/s bis hin zu 100 Gbit/s optimal. Die SINA L2 Box S 100G kann dabei sowohl in Punkt-zu-Punkt-Szenarien als auch als Kopfstation (Headend) für Aggregationslösungen eingesetzt werden.

Somit sind Netzbetreiber frei bei der Auswahl der SD-WAN Lösung im unverschlüsselten (roten) Netzwerkbereich. Zusätzlich dazu erhält der Anwender beim Einsatz der SINA L2 Box S eine vom jeweiligen SD WAN-Hersteller unabhängige, transparente VS-NfD-zugelassene Lösung für sicheren Datenaustausch Made in Germany.

Post-Quanten-Kryptografie

Und auch im Hinblick auf Post-Quantum Kryptografie (PQC) hat die SINA L2 Box S etwas zu bieten. Denn sie folgt bereits heute der BSI-Handlungsempfehlung zur „Migration zu Post-Quanten-Kryptografie“. Die SINA L2 Box S verwendet zur regelmäßigen Schlüsselableitung einen vorverteilten symmetrischen Langzeitschlüssel, der via PIN-geschützter Smartcard im Gerät zur Verfügung gestellt wird. Dadurch ist es möglich, den asymmetrischen Schlüsselaustausch zwischen zwei Geräten mit Hilfe eines verteilten Geheimnisses symmetrisch zu verschlüsseln.

Für die Kryptografie auf elliptischen Kurven bietet die SINA L2 Box S darüber hinaus die Möglichkeit von geheim gehaltenen Kurvenparametern. Dies verkleinert den Angriffsvektor gegen Attacken mit Quantencomputern, da sich die Kurvenparameter bei Kenntnis von drei Punkten auf der Kurve berechnen lassen.

Effizienter dank Layer2

Prinzipiell gibt es die Möglichkeiten Datenverbindungen auf verschiedenen Layern des OSI Modells herzustellen. Von Layer 1 (L1) spricht man, wenn die Verbindung direkt auf der physikalischen Ebene hergestellt wird (z.B. als Bitstrom bei einem WDM System). Von Layer 2 (L2) spricht man bei Ethernet-Verbindungen und von Layer 3 (L3) bei IP Verbindungen.

Je nach Bedarf der Applikationsumgebungen haben dabei Layer2 oder Layer3 Lösungen spezielle einsatzorientierte Vorteile. Als generelle Orientierungshilfe kann gelten, dass bei einer hohen Anzahl von Endpunkten mit kleinem Bandbreitenbedarf (z.B. VoIP Endpunkte oder mobile Zugänge) und einer nachgelagerten Aggregation an größeren Standorten oder mobilen Zugangspunkten eine Layer3-basierte Lösung Skalierungsvorteile hat.

Bei größeren Bandbreiten der Endpunkte, eher symmetrischen Topologien und einer kleinen bis mittleren Anzahl von Endpunkten, haben hingegen Layer2-basierte Lösungen Effizienzvorteile bei der Datenübertragung und im Betrieb.

Layer1-basierte Lösungen werden aktuell überwiegend bei Punkt-zu-Punkt-Verbindungen (z.B. WDM-Verbindungen) eingesetzt und stellen die Grundlage für die höheren Übertragungs-schichten dar.

Bei der Wahl der Verschlüsselungsebene gelten ähnliche Überlegungen. Der Haupteinsatzpunkt für Layer2 Verschlüsslung liegt bei hohen Verbindungsbandbreiten (> 1 Gbit/s) und einer kleinen bis mittleren Anzahl von Endpunkten (meist <100). Ein wesentlicher Vorteil ist dabei die Transport-effizienz. Bei der Layer2-Verschlüsselung wird in Summe über alle Verbindungen weniger Overhead hinzugefügt und damit die zur Verfügung stehende Nutzbandbreite vorteilhaft ausgenutzt.

Darüber hinaus bieten Layer2-Verbindungen zudem den Vorteil der Betriebseffizienz. Dabei bleibt bei der Layer2-Verschlüsselung die IP-Ebene unberührt und der Endanwender behält die volle Kontrolle über die IP-basierte Paketweiterleitung (IP based forwarding). Somit muss auch nicht jede IP-Verbindung einzeln verschlüsselt und folglich weniger Sicherheitsbeziehungen betrachtet werden. Zusätzlich dazu können jederzeit auch andere Routing- oder Forwarding-Technologien (SDN/SD-WAN) unabhängig von der gewählten Verschlüsselungslösung eingesetzt werden.

Weitere Informationen zu den secunet Produkten für sicheren Layer2- und Layer3-Datenaustausch finden Sie unter: **www.secunet.com/sina**