DATENBLATT

Wire-Speed-Verschlüsselungsmodule mit hoher Kapazität

Für die 6500 Packet-Optical Platform

Die Ciena 6500 Packet-Optical Platform ist eine kosteneffiziente Lösung zur Sicherstellung der Vertraulichkeit von Daten während der Übertragung. Sie unterstützt die flexible, protokollagnostische Wire-Speed-Verschlüsselung bei Übertragungsraten von 10G, 100G und 200G. Die einfache Bedienung und Administration ermöglicht eine schnelle Implementierung von Datenschutzstrategien für Ethernet, Fibre Channel, SDH/SONET und Optical Transport Network (OTN).

Die Ciena WaveLogic-Verschlüsselungslösung kombiniert bewährte Verschlüsselungstechnologien, die schon vielfach weltweit implementiert wurden, mit der Zuverlässigkeit der marktführenden 6500 Plattform, die von mehr als 600 globalen Betreibern eingesetzt wird. Die Lösung ermöglicht eine einfache Implementierung, da die Verschlüsselungsfunktionalität direkt in die Netzwerkkomponenten im Transportnetz integriert wird. Dies reduziert die Komplexität von Netzen, denn es müssen keine unterschiedlichen Verschlüsselungslösungen für verschiedene Applikationen verwaltet werden.

Zertifizierte Lösung für hohe Sicherheitsansprüche

Wie es dem Multi-Layer-Sicherheitsansatz von Ciena entspricht, ist die Verschlüsselung bei der Ciena WaveLogic-Verschlüsselungslösung immer aktiviert, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten im Netzwerk sicherzustellen. Die ständige Verschlüsselung des gesamten Datenverkehrs sorgt stets für die höchste Sicherheitsstufe. Zwar mag die Fähigkeit zum Ein- oder Ausschalten der Verschlüsselung zusätzliche Flexibilität bieten, aber ein einfacher menschlicher Fehler kann dann dazu führen, dass sensibler Datenverkehr unverschlüsselt über das Netz übertragen wird. Die Lösung wird von externen Institutionen validiert und zertifiziert, um sicherzustellen, dass eine standardisierte AES-Engine mit den entsprechenden Algorithmen implementiert wird. Es werden die höchsten anerkannten Sicherheitsstandards unterstützt, darunter Common Criteria und FIPS-Zertifizierung. Damit steht eine FIPS-zertifizierte AES-256-Verschlüsselungsengine mit standardbasierter Authentifizierung (wie beispielsweise X.509 Zertifikaten) zur Verfügung, die einen vereinfachten Betrieb aufgrund nahtloser Integration in vorhandene Unternehmens-PKIs ermöglicht.

Funktionen und Vorteile

- Wire-Speed-Verschlüsselungslösung mit extrem niedriger Latenzzeit, für hochsichere und transparente Kommunikation über die gesamte Übertragungsstrecke
- Protokollagnostische Verschlüsselung mit Flexibilität für die Unterstützung einer Vielzahl von Services
- Sichert alle wichtigen Daten während der Übertragung mithilfe einer FIPS-konformen Verschlüsselungslösung auf Basis des Advanced Encryption Standard (AES256)
- Zwei unterschiedliche Schlüsselsätze für die Authentifizierung und die Datenverschlüsselung, mit einer schnellen Schlüsselrotation im Sekundenbereich
- Nahtlose Integration in vorhandene Unternehmens-PKIs mit X.509-Authentifizierung auf Zertifikat-Basis
- Sicheres Management durch den Endbenutzer mithilfe des integrierten Management-Tools und damit Möglichkeit der Unterstützung von Encryption-as-a-Service in Carrier- oder Unternehmens-Infrastrukturen
- In der Praxis erprobte Verschlüsselungslösung, die bereits weltweit in Netzen in den Bereichen Finanzdienstleistung, Energieversorgung, Gesundheitswesen, Militär und Behörden eingesetzt wird

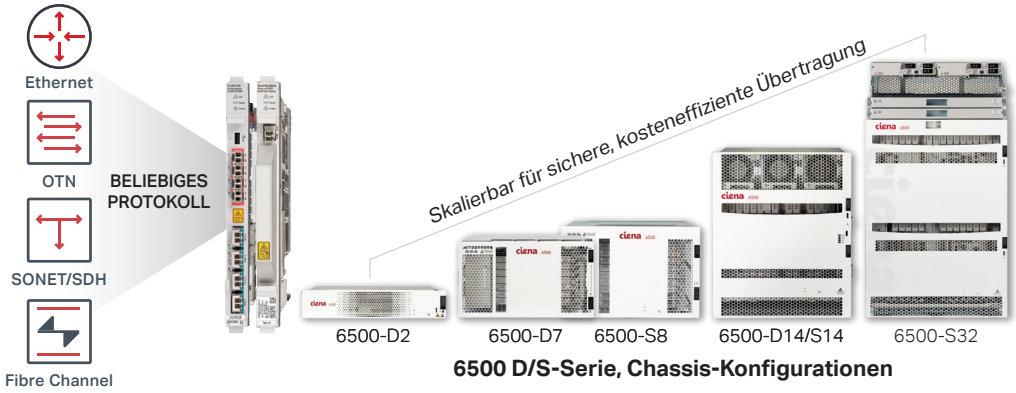

Abbildung 1: 6500 protokollagnostische Wire-Speed-Verschlüsselungslösung, skalierbar für alle Kundenanforderungen

Beispiellose Flexibilität

Aufgrund der Flexibilität des 6500 können Kunden die optimale Bauform für ihre individuellen Anforderungen in Bezug auf Kapazität, Platz- und Energiebedarf wählen, wodurch eine kosteneffiziente Übertragung verschlüsselter Daten gewährleistet ist. Die Lösung ist völlig protokollagnostisch – ein zusätzlicher Vorteil, da hierdurch eine Vielzahl flexibler Clients unterstützt wird, um unterschiedliche Applikationen bei sicherheitsbewussten Kunden zu unterstützen. Kunden können differenzierte Services implementieren, wenn niedrige Latenzzeiten und verschiedene Pfad- und Geräteschutzoptionen benötigt werden.

Encryption Testing and Certification
Kurzinformation herunterladen

Robuste Verschlüsselung

Zwei getrennte und voneinander unabhängige Schlüssel für die Authentifizierung und die Datenverschlüsselung bieten zusätzlichen Schutz. Das Rotationsintervall der Schlüssel ist äußerst kurz und beträgt nur wenige Sekunden. Die AES-256-Datensitzungsschlüssel werden automatisch ausgehandelt sowie sekündlich für jede Leitungsschnittstelle der Karte unabhängig voneinander aktualisiert, ohne dass Datenverkehr oder Durchsatz hiervon beeinträchtigt werden oder der Benutzer eingreifen muss. Betreiber können damit die neueste Generation von Public-Key-Verschlüsselungs-algorithmen implementieren, welche auch Elliptic Curve Cryptography (ECC) unterstützen. Damit ist eine gegenüber den Verschlüsselungssystemen der ersten Generation erheblich bessere Sicherung möglich.

Abbildung 2. 4x10G OTR mit Verschlüsse-lungsmodul

Wire-Speed-Verschlüsselung mit 10G

Mit dem 4x10G Optical Transponder (OTR), der nur einen Steckplatz benötigt, können Betreiber kostengünstig verschlüsselte 10G-Services anbieten. Dabei stehen durch die vier getrennten, protokollunabhängigen Leitungsschnitt-stellen insgesamt 40G zur Verfügung. Das Modul entspricht FIPS 140-2 Level 3 und bietet erweiterten Schutz gegen physische Manipulationen, denn die Schlüssel werden automatisch mit Nullen überschrieben, wenn eine Manipulation des Verschlüsselungsmoduls erkannt wird. Dies gilt selbst dann, wenn die Karte nicht eingesteckt ist.

Programmierbare WaveLogic-Verschlüsselung mit 100G oder 200G

Bei der Ciena WaveLogic-Verschlüsselungslösung wird die branchenführende kohärente WaveLogic-Technologie eingesetzt, um flexible Verschlüsselungslösungen mit hoher Kapazität zu implementieren. Die Basis hierfür ist das neue WaveLogic 3 (WL3) Extreme-Leitungsmodul. WL3 Extreme basiert auf den Funktionen von WL3 und zeichnet sich durch eine herausragende Leistung bei sämtlichen kohärenten Netzanwendungen aus. Möglich wird dies durch zusätzliche Modulationen sowie durch eine verbesserte Kompensation

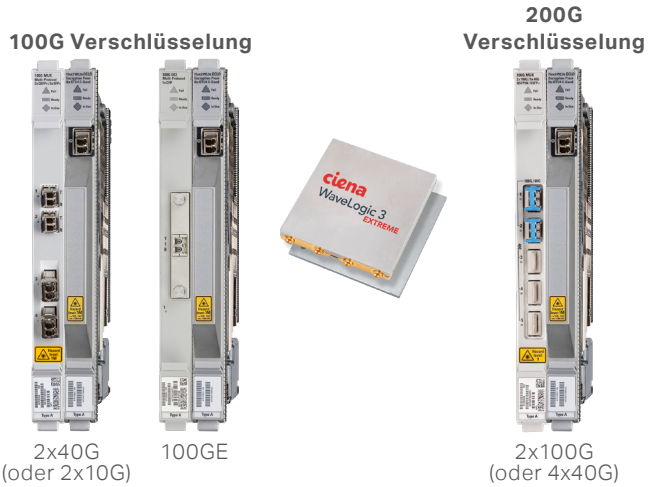

Abbildung 3. Beispiele für programmierbare 100G- oder 200G-Wire-Speed-Verschlüsselung mit dem WL3 Extreme-Leitungsmodul

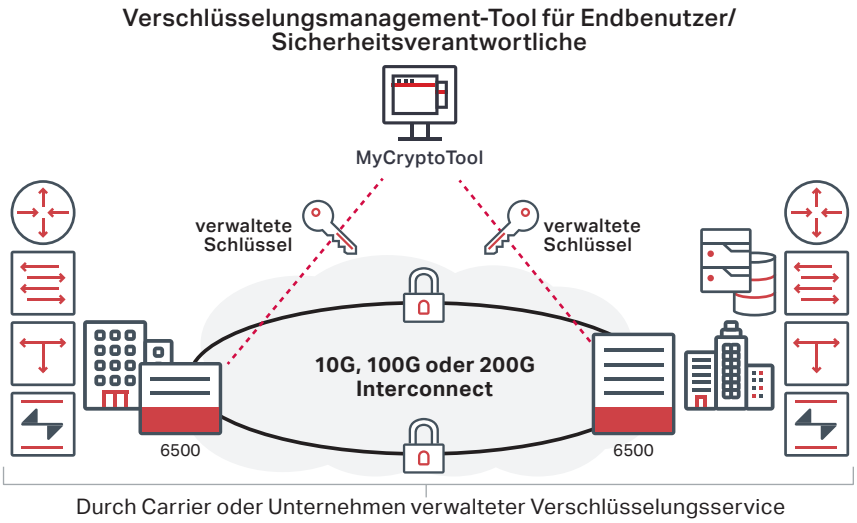

Abbildung 4. MyCryptoTool, die dedizierte Schnittstelle für das Verschlüsselungsmanagement

Data Security with Optical Encryption
Infografik jetzt herunterladen

linearer und nichtlinearer Fehler. Die technologisch führende Lösung adressiert alle Infrastruktur-Anforderungen, von Metro bis Langstrecke, und ermöglicht die Programmierung der Modulation durch Software; damit wird sowohl die 100G-Verschlüsselung mit QPSK-Modulation als auch die 200G-Verschlüsselung mit 16QAM-Modulation unterstützt – eine branchenweite Neuheit.

Durch Integration des WL3 Extreme-Leitungsmoduls in unterschiedliche Client-Schnittstellen können flexible Lösungen implementiert werden, welche die jeweiligen Datenverkehrsanforderungen unterstützen – egal, ob die Übertragungsservices 10G, 40G oder 100G erfordern. Bei wachsenden Anforderungen kann das WL3 Extreme-Leitungsmodul so programmiert werden, dass eine verschlüsselte Datenübertragung mit 200G ermöglicht wird – einfach durch Hinzufügen einer weiteren Client-Karte. Weiterhin besteht die Möglichkeit, verschlüsselte Services mit hoher Kapazität mithilfe der Hybrid-Packet-/OTN-Fabric des 6500 zu implementieren – damit können Netzressourcen äußerst effizient genutzt werden.

Verschlüsselungsmanagement leicht gemacht

Zur 6500 WaveLogic-Verschlüsselungslösung von Ciena gehört auch MyCryptoTool, eine Benutzerschnittstelle für das Verschlüsselungsmanagement, das speziell für das verteilte Management von Netzen entwickelt wurde. Damit besteht die Möglichkeit zur unabhängigen Verwaltung von Sicherheitsparametern und Alarmen bei Services mit 10G, 100G oder 200G – sowohl durch den Carrier als auch durch den Unternehmenskunden. MyCryptoTool ist eine benutzerfreundliche Schnittstelle, welche eine sichere Verbindung zum kryptografischen Modul herstellt und gegenseitige Authentifizierung bietet, wodurch der Zugriff auf autorisiertes Sicherheitspersonal beschränkt wird.

Die Ciena WaveLogic-Verschlüsselungslösung kombiniert einen hohen Grad an Flexibilität und Sicherheit mit einfachen Betriebsfunktionen und ermöglicht damit kosteneffiziente, protokollagnostische Verschlüsselungslösungen mit extrem niedriger Latenzzeit für 10G, 100G und 200G. Damit können praktisch alle aktuellen Web-Scale-Applikationen effizient geschützt werden.

Wire-Speed-Verschlüsselungslösung
Applikationsschrift
Jetzt herunterladen

Technische Daten

Schnittstellenkarte	**4x10G OTR mit Verschlüsselung**	**WaveLogic 3 Extreme Leitungsmodul mit Verschlüsselung**
Systemanforderungen	Geeignet für alle Chassis der 6500 S/D-Serie	Geeignet für alle Chassis der 6500 S/D-Serie, außer 6500-D2
Port-Format **Unterstützte Client-seitige Schnittstellen**	STM-64/OC-192 10GbE LAN, 10GbE WAN FC400, FC800, FC1200 OTU2, OTU2e	STM-64/OC-192 10GbE LAN, 10GbE WAN, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
Unterstützte Leitungsschnittstellen	OTU2 OTU2e	100G kohärent (QPSK); 1 x OTU4 200G kohärent (16QAM); 2 x OTU4
Redundanzoptionen	1+1-Leitungsschutz 1+1-Client- und Equipment-Schutz	1+1-Leitungsschutz 1+1-Client- und Equipment-Schutz
FEC-Modi	RS-8 FEC, UFEC und OFF gemäß G.709	Soft FEC
Umgebungsbedingungen Betriebstemperatur Relative Feuchte Höhe	 +5 °C bis +40 °C (+41 °F bis +104 °F); -5 °C bis +55 °C (+23 °F bis +131 °F) kurzfristig – für 6500-D2/D7/S8/D14/S14 -5 °C bis +50 °C (+23 °F bis +122 °F) kurzfristig – für 6500-S32 5 % bis 85 % (nicht kondensierend) 13.000 Fuß; 4000 m	
Technische Merkmale	288 mm (H) x 25 mm (B) x 237 mm (T) 11,34 Zoll (H) x 0,99 Zoll (B) x 9,34 Zoll (T)	
Sicherheitsfunktionen	• NIST-zertifizierte AES-256-Verschlüsselungslösung für die Datenverschlüsselung • Algorithmen für Elliptic Curve Cryptography (ECC) • Diffie-Hellman-Key-Negotiation (einschließlich Elliptic Curve) • Unterstützt X.509-Zertifikate für die Authentifizierung • Unterstützung für Certificate Revocation List (CRL) • Unterbrechungsfreier, sekündlicher AES-256-Schlüsselaustausch • Schnittstelle für das Verschlüsselungsmanagement, mit sicherer Authentifizierung • Unterstützung für Radius-Authentifizierung • TACACS + AAA • SNMPv3-Unterstützung	
	• 2048-Bit-RSA-Zertifikate • Elliptic-Curve-Zertifikate	• Elliptic-Curve-Zertifikate
Zertifizierungen	• Common Criteria Network Device Collaborative Protection Profile • BSI (Bundesamt für Sicherheit in der Informationstechnik) • FIPS 140-2 Level 3 – Zertifikat Nr. 2379, Nr. 2635 • FIPS 197 – AES–256 – Zertifikat Nr. 2963, Nr. 2964, Nr. 3599, Nr. 3600 • IBM GDPS • EMC, Brocade	• Common Criteria Network Device Collaborative Protection Profile • BSI (Bundesamt für Sicherheit in der Informationstechnik) • FIPS 140-2 Level 2 – Zertifikat Nr. 2697, Nr. 2843 • FIPS 197 – AES–256 – Nr. 3601, Nr. 3602, Nr. 4231, Nr. 4232, Nr. 5241 • IBM GDPS • EMC, Brocade

Nehmen Sie jetzt Kontakt zu Ciena auf