

Die Verbreitung von Multi-Gigabit Datennetzen und Speichernetzen nimmt rasant zu. Insbesondere wegen der breiten Verfügbarkeit von Dark Fiber und WDM Technologien können auch sehr schnelle WAN Backbones auf einfache Weise realisiert werden.

Mit der Verbreitung der Technik steigt aber auch das Risiko, dass vertrauliche Daten im WAN abgehört oder sogar manipuliert werden können. Möglicherweise können Dritte sogar vollen Zugriff auf die internen Netzwerkstrukturen erhalten.

Darum muss der über öffentliche Leitungswege geführte Teil des Netzwerks gegen solche Angriffe geschützt werden. Eine hohe Akzeptanz der Sicherheitslösung wird erreicht, wenn keine Änderungen der Netzwerkstruktur und der Betriebsabläufe notwendig sind.

Der **ATMedia 10G Encryptor** schützt die SONET/SDH Infrastruktur durch einfaches Einsetzen in die WAN Leitung. Die Hardware-Verschlüsselung auf Netzwerk-Layer 1 garantiert eine vollkommen transparente Arbeitsweise bezüglich höheren Protokollen.

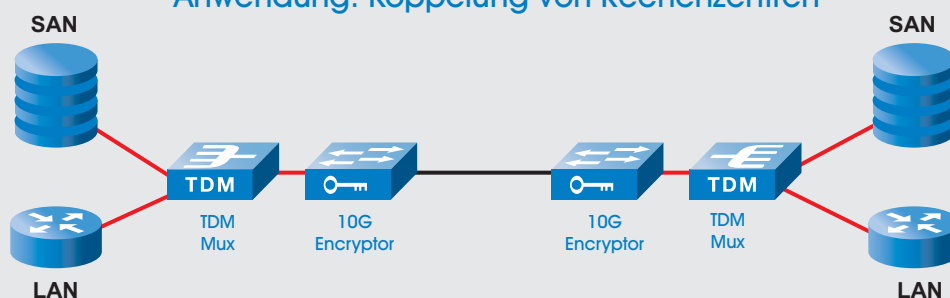
ATMedia 10G SONET Encryptor



Highlights

- Voll-Duplex Verschlüsselung bei 10 Gigabit SONET/SDH Line Rate
- Kein Verschlüsselungs-overhead
- Netzwerk-Integration ohne Änderung der Konfiguration
- Wartungsfreier Betrieb
- Austauschbare XFP Interfaces
- Zugelassen für Verschlusssachen durch das BSI (VS-NfD)

Anwendung: Koppelung von Rechenzentren



- Aggregation von Storage und Ethernet Services in einen OC-192 Link
- Verschlüsselung des OC-192 SONET/SDH Links mit dem 10G Encryptor
- Vorteile
 - Kosten-Effizient
 - 1G Ethernet, 1G, 2G und 4G Fibre Channel
 - TDM Systeme sind von verschiedenen Herstellern verfügbar
 - Datacenter Zertifizierungen sind für die TDM Systeme verfügbar

Technische Daten

Leistungsdaten

- Echtzeit Verschlüsselung von 10G SONET/SDH STM-64/OC-192 links
- Voll-Duplex Line-Speed Verschlüsselung ohne Overhead
- Schlüsselwechsel ohne Unterbrechung des Links
- Latenz: 10G: ≤ 0,004ms je Gerät

Verschlüsselungstechnologie

- AES (256 Bit) Verschlüsselungsverfahren mit CBC Block Modus
- Schlüsselerzeugung durch Hardware Zufallszahlengenerator
- Schlüsselaustausch über Diffie-Hellman ECC Verfahren (DH-ECKAS)
- Konform zu den Anforderungen von FIPS 140-2 L3 und CC EAL3
- Zugelassen vom BSI für VS-NfD, NATO und EU restricted

Schlüssel Management

- Ad-hoc Authentisierung
- Manipulationsgeschützte Schlüsselspeicherung
- Automatischer Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall
- Autonomer Betrieb ohne externes Schlüsselmanagement

System Management

- Konfiguration über serielle Konsole (RS-232/V.24) oder Secure Shell (SSH) Netzwerkzugang (Out-of-Band Ethernet RJ45-10/100BT)
- Integrierte Leitungs- und Betriebsüberwachung
- Audit und Event Logging
- Syslog Support
- Abfrage des Betriebszustandes über SNMP (V2c/V3 authpriv)
- Überwachung des Linksstatus mittels ATMedia CryptMon

Netzwerk

- Kompatibel zu SDH und SONET
- Transparente Durchleitung des SDH Overheads
- Durchleitung und Aufbereitung und des Taktes (3R)
- Optical Loss pass-through (Link Loss Carry Forward)
- Line Interfaces

XFP-Module
 XFP MM LC (62,5/125μ)
 XFP SM LC (9/125μ) SR/IR/LR
 XFP DWDM/CWDM

Hardware

- Arbeitstemperatur: 1°C - 40°C
- Luftfeuchtigkeit: 10% - 85%, nicht kondensierend
- Gehäuse: 482,6mm (19") 2HE, H: 88mm, B: 430mm, T: 370mm, G: 10kg
 Redundante Hot-Swap Stromversorgung
 110-240V AC 50-60Hz oder -48V DC, 115W
 Tamper resistentes Design
- Konformität: CE, FCC

The ATMedia systems and related documentation are subject to continuous improvement. Therefore ATMedia reserves the right to change documentation without notice.