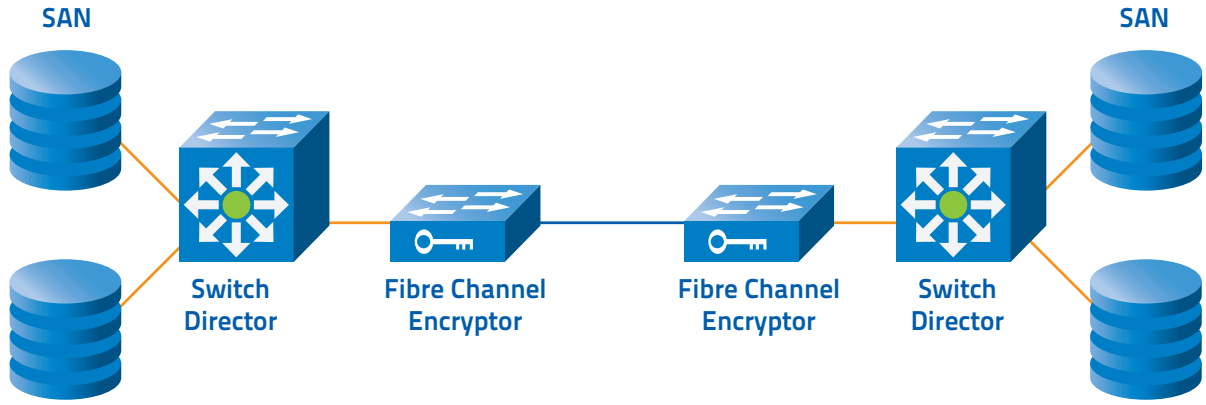
atmedia
secure data communication

Fibre Channel Encryption

atmedia Fibre Channel Encryptor

Storage Area Networks are the backbones of today's computing infrastructure. Since they connect servers to their storage and backup systems, most sensitive data will be transferred over these networks. In a local environment, standard security measures like zoning and physical access restrictions might be sufficient. For a SAN that spreads over several distant locations however there exists a high risk of tapping and manipulation of most critical data. The SAN technology Fibre Channel is used for local storage connectivity as well as for connecting remote systems for business continuity scenarios. A SAN extension can be easily realized by connecting several local Fibre Channel networks over Dark Fiber or WDM technology. The atmedia Fibre Channel Encryptor enables the protection of this distributed Fibre Channel SAN by a very simple integration into the existing Fibre Channel structure. It encrypts the payload between the switches and thus effectively prevents eavesdropping and manipulation of the valuable storage data. The hardware encryption works at network layer 2 and does not cause any measurable effect on SAN operation.

Application scenario



Highlights

- Strongest crypto technology available (AES, ECC)
- Full-duplex encryption at line rate (1gbps/2gbps)
- Encryption of Fibre Channel E-ports
- No encryption overhead
- Network integration without any change of infrastructure (bump in the wire)
- Maintenance-free operation
- Hot-swappable SFP line interface support
- Compliant to the requirements of FIPS 140-2 L3 and CC EAL4

atmedia GmbH
Science Park 1
66123 Saarbrücken
GERMANY

Tel: +49 681 84 24 77
Fax: +49 681 84 24 81

crypt@atmedia.de
www.atmedia.de

atmedia
secure data communication

Technical Data

SAN Security

Performance
▪ Real-time encryption of 1G/2G Fibre Channel E-Ports
▪ Full-duplex line-speed throughput independent of packet size
▪ Key changes without interruption of traffic
▪ Latency per device: ≤ 0,010ms

Crypto Technology
▪ AES (256 bit) encryption with CBC block mode
▪ Key generation with hardware random source
▪ Key exchange with Diffie-Hellman ECC algorithm (DH-ECKAS)
▪ Compliant to the requirements of FIPS 140-2 L3 and CC EAL3

Key Management
▪ Ad-hoc device authentication
▪ Tamper resistant key storage
▪ Automatic time triggered change of master keys and group keys
▪ Autonomous operation without external key management

System Management
▪ Configuration via serial console (RS-232/V.24) or Secure Shell (SSH) network access (out-of-band Ethernet RJ45-10/100BT)
▪ Integrated monitoring of network status and operation
▪ Audit and event logging
▪ Syslog support
▪ Remote monitoring via SNMP (V2c/V3 authpriv)
▪ Link monitoring via atmedia CryptMon

Network
▪ Compatible to 1G/2G Fibre Channel E-Port
▪ E-Port / Inter Switch Link (ISL) Interface
▪ Optical Loss Pass-through

Hardware
Operating temperature: 1°C - 40°C
Relative humidity: 10% - 85%, non condensing
Chassis: 482,6mm (19") 1RU, H: 44mm, W: 430mm, D: 320mm
Weight: 7kg
Redundant Hot-Swap PSU: 110-240V AC 50-60Hz or -48V DC, 90W
Tamper resistant design

Line Interfaces
SFP-modules
SFP MM LC (62,5/125µ)
SFP SM LC (9/125µ) SR/IR/LR
SFP DWDM/CWDM

Conformity
▪ CE, FCC

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

atmedia GmbH
Science Park 1
66123 Saarbrücken
GERMANY

Tel: +49 681 84 24 77
Fax: +49 681 84 24 81

crypt@atmedia.de
www.atmedia.de