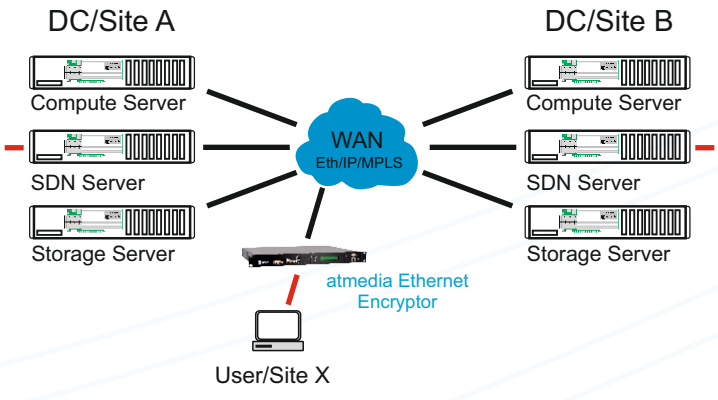
cryptoNIC: Hochsichere SDN und Cloud Verschlüsselung bis 100G

Der kontinuierliche Anstieg von Virtualisierung und softwarebasierten Netzwerkfunktionen belastet die Verarbeitungskapazität von Server-CPUs erheblich. Intelligente Netzwerkkarten (SmartNICs) werden zu einer immer beliebteren Methode, um intensive Paketverarbeitungsaufgaben von Servern auszulagern.
Die atmedia cryptoNIC kombiniert die intelligente Netzwerkkarte mit einer vom BSI zugelassenen Sicherheitsfunktion. Die Karte basiert auf dem modernen PCIe (Peripheral Component Interconnect Express) Standard zur direkten, extrem schnellen Datenübertragung zwischen Prozessor (CPU), RAM-Speicher und Peripheriekomponenten.
Die Layer 2 und Layer 3 Netzwerkverbindungen zwischen typischen Servern bzw. Servern und Endgeräten können bei Einsatz der atmedia cryptoNIC zuverlässig und ohne Qualitätseinbußen gesichert werden. Das Einsatzgebiet erstreckt sich dabei von der Verschlüsselung von Punkt-zu-Punkt Verbindungen bis hin zur Absicherung komplexer SD-WAN und Cloud-Infrastrukturen. Die Systeme eignen sich insbesondere für die Realisierung von hochverfügbaren Szenarien mit geringer Latenz.
Die atmedia cryptoNIC realisiert die Netzwerk- und Verschlüsselungsfunktionalität mittels eigenentwickelter FPGA-Hardware. Durch den AES-GCM Integritäts- und Replay-Schutz der Daten- und Kontrollebene arbeitet die cryptoNIC wie eine „perfekte Firewall“. Aufgrund der Datenverarbeitung in Leitungsgeschwindigkeit sind die Systeme immun gegen DDoS Angriffe. Durch diesen Schutz gegen aktive Angriffe erfolgt eine signifikante Verbesserung der Cyber-Resilienz kritischer Infrastrukturen.

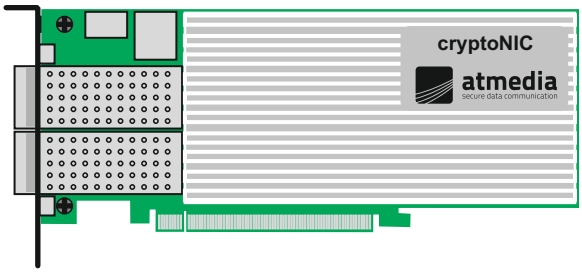
Anwendungsbeispiele

Integration in ein SD-WAN oder Firewall System

Integration in ein Cloud System



atmedia cryptoNIC 100G



Highlights

- Crypto/Netzwerk Offloading in FPGA Hardware
- Kompatibel zum atmedia Ethernet Encryptor
- Kompatibel zu marktüblichen Server-Systemen
- Stärkste verfügbare Verschlüsselungstechnologie
- Quantenresistente Implementierung
- Hardware-Zufallszahlenerzeugung
- Layer 2 oder Layer 3 Verschlüsselung
- Sichere SD-WAN Underlay Verschlüsselung
- Minimaler Overhead bei sicherem Betrieb
- Keine Änderung der Infrastruktur notwendig
- Unterstützung bestehender Redundanzszenarien
- Wartungsfreier Betrieb
- Sehr geringe Leistungsaufnahme (Green IT)
- Zugelassen für Verschlusssachen durch das BSI (VS-NfD, EU RESTRICTED, NATO RESTRICTED)
- Made in Germany

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

Technische Daten

atmedia cryptoNIC

Gerätetypen	
• cryptoNIC 10G:	10G mit zwei SFP+ Interfaces
• cryptoNIC 100G:	25G/100G mit zwei QSFP28 Interfaces

Netzwerkintegration lokale (rote) Seite
• Linux Netzwerk Device-Treiber für Host-Anbindung (Open-Source)
• Optional (lokal): Verwendung der zweiten SFP/QSFP Schnittstelle

Leistungsdaten
• Ethernet (Layer 2) und IP (Layer 3) Verschlüsselung im Punkt-zu-Punkt-, Punkt-zu-Multipunkt- oder Multipunkt-Modus
• Mandantenfähige Gruppenverschlüsselung (max. 1000 Peers)
• Echtzeit Verschlüsselung in FPGA Hardware
• Durchsatz unabhängig von der Paketgröße
• Sehr niedriger Stromverbrauch (Green IT)
• Latenz: < 5µs

Netzwerk
• Kompatibel mit E-Line, E-Tree, E-Lan, VPLS, VPWS und anderen Ethernet Services
• Unterstützung von Jumbo Frames, optionale Fragmentierung
• IP-Tunnel Modus: Layer 2 über IPv4 oder IPv6 (IP oder UDP) Durchsatz bei kleinen Paketen über 97% der Netzbandbreite
• Link Loss Carry Forward/Optical Loss Pass Through
• Traffic Flow Security Modus verhindert das Erkennen und die Analyse der verschlüsselten Kommunikation sowie verdeckte Kanäle
• Schutz gegen aktive Angriffe (Denial of Service) durch hardware-basierte Paketfilterung und Absicherung der Kontroll-Schicht
• Einfache und sichere IPv6 Unterstützung
• Interoperabel zu verbreiteten Netzwerkprodukten

Optionen
• Interface Module für LWL bzw. QSFP Adapter
• Slotblende für PCIe Full-Height
• Optionale Lizenzen für höhere Verschlüsselungsleistungen
• Optionale Lizenzen für custom ECC, custom AES und TFS

Verschlüsselungstechnologie
• AES-GCM (256 Bit) Verschlüsselungsverfahren (128 Bit Tag)
• Integritäts- und Replay-Schutz über Galois Counter Modus (GCM)
• Schlüsselerzeugung durch Hardware Zufallszahlengenerator
• Schlüsselaustausch über Diffie-Hellman ECC (ECDH)
• Konform zu den Anforderungen von FIPS 140-2 L3 und CC EAL4
• Zugelassen vom BSI für VS-NfD, NATO und EU RESTRICTED

Schlüsselmanagement
• Ad-hoc Authentisierung zum Registrieren von Gegenstellen
• Manipulationsgeschützte Schlüsselspeicherung
• Built-in Schlüsselserver zur Verteilung von Gruppenschlüsseln
• Automatischer, unterbrechungsfreier Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall

Systemmanagement
• Konfiguration über Konsole (USB-serial) oder Secure Shell (SSH) Netzwerkzugang
• Integrierte Leitungs- und Betriebsüberwachung
• Audit und Event Logging
• Abfrage des Betriebszustandes über SNMP (V2c/V3 authpriv)
• Überwachung des Linkstatus mittels atmedia CryptMon

Hardware	
• Arbeitstemperatur:	1°C - 40°C
• Luftfeuchtigkeit:	10% - 85%, nicht kondensierend
• PCIe Karte:	Tamper resistentes Design HHHL PCIe Board Gen3x16
• Stromversorgung:	cryptoNIC 10G: 25W cryptoNIC 100G: 50W

Konformität
• CE, FCC

Die atmedia Systeme sowie die zugehörige Dokumentation werden ständig auf dem neuesten Stand der Technik gehalten. atmedia behält sich daher vor, Änderungen jederzeit und ohne vorherige Ankündigung durchzuführen.

Aktueller Firmware-Stand: 3.4.0

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