ZYBERSAFE

DATA SHEET

Zybersafe TrafficCloak – Ethernet Encryption

Ethernet Encryption

Securing Data in Use, distinguish from Data at Rest by encryption at the Data Link Network Layer (L2), ensures superior network performance, simplifies network operations and reduces the overall cost of data protection. Zybersafe ethernet encryption products offer a transparent, wire-speed encryption service using the internationally recognized Advanced Encryption Standards (AES) algorithm for securing private information. The AES algorithm is implemented in its most secure version, 256-Galois Counter Mode, ensuring Authentication, Data-Integrity and protection against replay attacks.

The Zybersafe ethernet encryption product is factory paired and key pre-configured with keys, 100% randomly generated from the product's built-in HW Random Number Generator, no need for annoying, cumbersome key management and associated security risk.

Network management functionality is implemented and provided at a minimum level, supporting transmit-only SNMP status traps each 5 seconds to maximize security.The product's network ports come with high media flexibility with pluggable SFP/SFP+ interfaces for media specific transceiver modules and for direct-attach cables to enable connectivity to diverse 1, 10 and 100 GbE fiber and copper media performance solution. Easy to implement and ready to use within a reasonable budget.

Key Features

- Strongest crypto technology available, AES256-GCM
- Full-Duplex real-time encryption
- Keys are not user manageable/accessible
- Key generation from HW RNG
- Man-in-the-middle and replay protection of transmitted data
- Authentication and data integrity secured
- Supports 1G, 10G or 100G Ethernet point-to-point links
- Encryption of unicast, multicast and broadcast traffic
- Network integration without any change of infrastructure (virtual wire)
- Highly scalable
- No impact on existing redundancy mechanisms
- Approved by Danish Centre for Cyber Security
- CE compliant

Performance

- Full-Duplex real-time layer 2 encryption
- Encryption independent of packet (size and content)
- Key changes without interruption of traffic
- Support of 1G, 10G or 100G Ethernet line interfaces
- Latency ≤ 0,05ms

Key management

- Keys are not user-manageable/accessible
- Built-in HW RNG for master key generation
- Automatic time triggered change of master keys
- Tamper resistant key storage
- Continues device authentication

Management

- No management needed
- Monitoring via SNMP traps from status port

Network

- Supports 1G, 10G or 100G Ethernet point-to-point links
- Support of Jumbo frames
- Support of 1G, 10G or 100G Ethernet line interfaces
- Network integration w.o. any change of infrastructure
- No impact on existing redundancy mechanisms

LAN and WAN Interfaces

- 1Gbps model: SFP interfaces
- 10Gbps model: SFP+ interfaces
- 100Gbps model: QSFP28 interfaces

Status port:

- 1000Base-T RJ-45

Encryption

- AES-GCM (256 bit) encryption
- Encryption of unicast, multicast and broadcast traffic
- Authentication and data Integrity secured
- Man-in-the-middle-attack and replay protected by Galois Counter Mode (GCM)

Hardware

- Operating temperature: 1°C - 40°C
- Relative humidity: 10% - 85%, non condensing
- 482.6mm (19“) 1RU, H: 44mm, W: 430mm, D: 320m
- Weight: 7.5 kg. including packaging
- Redundant Hot-Swap PSU AC or DC:
    - AC: 100-240V, 50-60Hz
    - DC: 40-72V
- Power consumption: typical 35W
- Battery Life Time:
    - Storage: 3 years
    - In service: 10 years

Conformity

- CE
- Approved by Centre for Cyber Security for use in Denmark for protection of information classified: TIL TJENESTEBRUG, NATO RESTRICTED, and EU RESTRICTED
- Designed to comply with requirements of Common-Criteria EAL4
- Designed to comply with requirements of FIPS 140-2 L3