Cipher

GOST* 28147-89

Deals With the Challenges

a hardware VPN gateway provides concurrent traffic processing in the following modes:

- *encryption:* data acquisition from a secure network interface, encryption, cryptographic checksum verification, encapsulation and forwarding packets through an open network interface,
- *decryption:* data acquisition from an open network interface, de-encapsulation, decryption, cryptographic checkvalue and forwarding packets through a secure network interface.

Provides Key Features

- encryption/decryption of IP-packets and prevention of data diddling at speeds up to 20 Gbs,
- while encrypting, the device uses a unique packet encryption key generated from the packet counter and a master key /password-encryption/ of the used tunnel,
- the device generates a data encryption key and a message authentication code for each IP-packet.

Is an Ethernet Encryption and VPN-enabling Device

Network packets processing by an encryption gear implies the ability to operate in the GOST 28147-89 format:

- MAC-mode – Message Authentication Code algorithm,
- CFB-mode – cipher feed back mode.

*Russian Federal Standard

OPTIONS

- network interfaces installation – **MAC** and **IP**-addresses, aggregation parameters;
- list of protected subnets for encryption – up to **2 048 routes**;
- list of used tunnels* – up to **512 tunnels**;
- a set of key information – up to **512 sets**, one per tunnel:

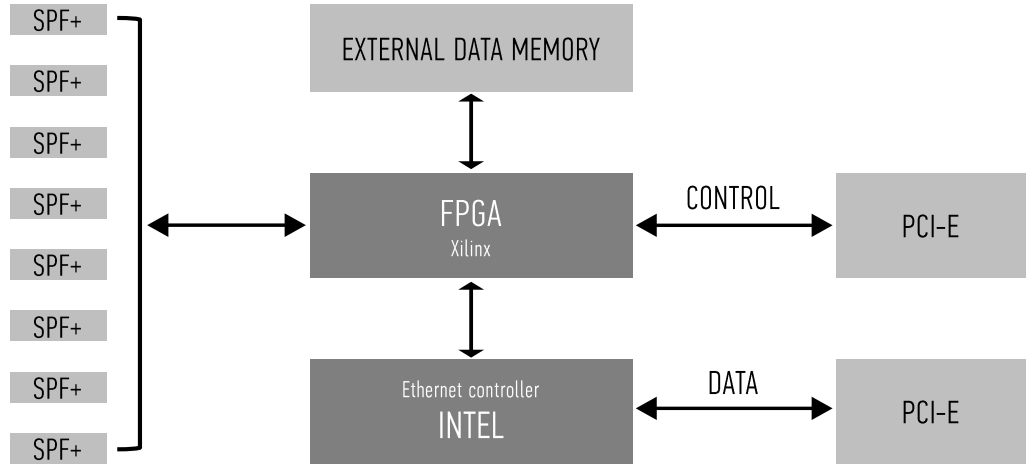
- 256-bit encryption master key,
- 64-bit encryption initialization vector,
- 64-bit decryption initialization vector,
- selection mode for a replacement node,
- IP address of the remote point that will decrypt the packets,
- 32-bit tunnel identifier;

- routing table for packet recipients – up to **128 routes**;
- dynamic MAC address table with ARP protocol support – up to **256 entries**.

**Interconnections between two secure subnets*

TECHNICAL DATA

- overall streaming rate: **20 Gb/s** for packet size more than 800 bytes;
- support for **JUMBO**-packets – up to 4 KB;
- ability to integrate physical Ethernet ports into logical channels / with **LACP** support according to 802.1AX /;
- off-line encryption and decryption of packets,
- encryption and decryption with further processing in the CPU.



control interfaces

network interface	8 network interfaces SFP+ (1,10 Gb/s)
data exchange interface	PCIe 8x
module control interface	PCIe 8x